THE
CARTER CENTER

Misión Técnica del Centro Carter
Elecciones Presidenciales
3 de diciembre de 2006
Venezuela

Informe Final

Waging Peace. Fighting Disease. Building Hope.

The Carter Center strives to relieve suffering
by advancing peace and health worldwide; it seeks
to prevent and resolve conflicts, enhance freedom and
democracy, and protect and promote human rights worldwide.

Misión Técnica del Centro Carter
Elecciones Presidenciales
3 de diciembre de 2006
Venezuela

Informe Final

THE
CARTER CENTER

One Copenhill
453 Freedom Parkway
Atlanta, GA 30307
(404) 420-5188
Fax (404) 420-5196
www.cartercenter.org

Diciembre 2007

Índice

Personal y Equipo Técnico del Centro Carter

Equipo técnico del Centro Carter

Ingo Boltz (Alemania), Tecsel S.A., Consultor voto electrónico del Centro Carter, Argentina.

David Carroll (Estados Unidos), Director del Programa para la Democracia, Centro Carter, Estados Unidos.

Avery Davis-Roberts (Estados Unidos), Asociada al Programa para la Democracia, Centro Carter, Estados Unidos.

Richard DeMillo (Estados Unidos), Decano, *College of Computing, Georgia Institute of Technology*, Estados Unidos

Marcelo Escolar (Argentina), Tecsel S.A., Consultor voto electrónico del Centro Carter, Argentina.

Bill Gallery (Estados Unidos), Director de Programa, *Democracy International*, Estados Unidos.

Kristin García (Estados Unidos), Coordinadora Adjunta de los Programas para la Democracia y para las Américas, Centro Carter, Estados Unidos.

Herman Ruddijs (Holanda), Gerente Comercial de Proyectos, Departamento de Desarrollo Empresarial, Sdu Uitgevers, Holanda.

Hector Vanolli (Argentina), Director de la oficina de Venezuela del Centro Carter, Venezuela

Ethan Watson (Estados Unidos), Pasante, Programa para la Democracia, Centro Carter, Estados Unidos.

Personal del Centro Carter

Josefina Blanco (Venezuela), Encargada de Prensa, Centro Carter, Venezuela.

Glory Melendez (Venezuela), Contadora, Centro Carter, Venezuela.

Jacqueline Mosquera (Venezuela), Gerente de oficina, Centro Carter, Venezuela.

Términos y Abreviaturas

AAA	*Authentication, Authorization and Accounting* [Autenticación, Autorización y Registro]
AC	Autoridad de Certificación
AES 256bit	En criptografía, *Advanced Encryption Standard* (AES) es un estándar de cifrado con una longitud de claves de 256 bits.
AFIS	*Automated Fingerprint Identification System* [Sistema automático de identificación de huellas dactilares]
BIOS	*Basic Input/Output System* [Sistema básico de entrada-salida]
CANTV	Compañía Anónima Nacional de Teléfonos de Venezuela (CANTV)
CDMA	*Code-Division Multiple Access* [acceso múltiple por división de código], una tecnología celular digital
CNE	Consejo Nacional Electoral
CRCE	Comisión de Registro Civil y Electoral
CPU	*Central Processing Unit* [Unidad central de procesamiento]
CTC	Centro de Transmisión de Contingencia
DLL	Dynamic Line Library [Bibliotecas de Enlace Dinámice]
DOM	*Disk on module*, una alternativa para los discos rígidos tradicionales
DRE	*Direct Recording Electronic* [Votación electrónica directa]
IDS	*Intrusion-detection system* [sistema de detección de intrusiones]
IP address	*Internet Protocol address*. Un identificador para una computadora o dispositivo en una red TCP/IP
IPS	*Intrusion-prevention system* [sistema de prevención de intrusiones]
IPSec	*IP Security*, una serie de protocolos desarrollados por el IETF para asegurar el intercambio de paquetes a nivel del IP
IU	Interfaz de usuario
JNE	Junta Nacional Electoral
MAC address	*Media Access Control address* (dirección de control de acceso al medio de un dispositivo de red)
MD-5, SHA-I, SHA-256	Algoritmos *hash*
MFT	*Master File Table*, [tabla maestra de archivos], un componente del sistema de archivos NTFS
NTFS	*New Technology File System*, uno de los sistemas de archivos diseñado para el sistema operativo Windows NT
Puerto serial / Puerto PS/2 / Puerto Ethernet / Puerto USB	Interfaces para conectar dispositivos externos a una computadora
RADIUS	*Remote Authentication Dial-In User Service*, un sistema de autenticación y autorización.
RAS	*Remote Access Server* [Servidor de acceso remoto]
RJ-45	Forma abreviada de *Registered Jack-45*, una interfaz física con ocho conexiones eléctricas para conectar las computadoras a redes de área local, especialmente Ethernets
RPV	Red privada virtual
SPI	*Stateful Packet Inspection* [inspección de paquetes de datos]
SSL/TLS	*Secure Sockets Layer* / *Transport Layer Security* (protocolos de seguridad).
TICs	Tecnologías de la Información y la Comunicación

Agradecimientos

El Centro Carter desea expresar su agradecimiento al Consejo Nacional Electoral (CNE) de la República Bolivariana de Venezuela por invitarlo a enviar una misión técnica especializada para observar el funcionamiento del sistema automatizado de votación durante las elecciones presidenciales del 3 de diciembre de 2006. De igual forma, el Centro Carter desea agradecer al gobierno de Irlanda, cuyo generoso apoyo financiero facilitó el trabajo de observación de la Misión.

El Centro Carter desea asimismo agradecer a las misiones de observación de la Unión Europea y la Organización de Los Estados Americanos por su estrecha colaboración durante todo el período electoral. El Centro Carter quisiera igualmente expresar su reconocimiento a los grupos de observación y asociaciones civiles nacionales, que desempeñaron un papel activo en esa elección.

El Centro Carter desea también hacer extensivo su agradecimiento a Richard DeMillo, Bill Gallery y Herman Ruddijs, quienes tuvieron la mejor disposición para viajar a Caracas pese a haber sido invitados con escasa antelación, y sin cuya presencia esta Misión no hubiera sido posible. Un especial agradecimiento se dirige a Marcelo Escolar e Ingo Boltz, quienes oficiaron de asesores técnicos a largo plazo durante todo el proceso de observación, y cuyo trabajo en circunstancias a veces difíciles constituyó la base para la tarea de la Misión.

La misión técnica especializada del Centro Carter tampoco hubiera sido posible sin el intenso trabajo y la dedicación del Representante del Centro Carter en Venezuela, Héctor Vanolli, quien trabajó sin descanso en Caracas para sentar los fundamentos del trabajo del equipo, con el apoyo crítico y la asistencia de Jacqueline Mosquera, Glory Melendez y Josefina Blanco.

En Atlanta, la Directora del Programa para las Américas del Centro Carter, Jennifer McCoy, brindó orientación y consejo permanentes, aportando su talento y experiencia, lo que resultó esencial para el proyecto. Kristin Garcia soportó largas horas de trabajo con permanente afabilidad y buen humor, y la presencia de Ethan Watson demostró ser indispensable en Caracas.

Finalmente, el Centro Carter desea agradecer especialmente a David Carroll y Avery Davis-Roberts, del Programa para la Democracia del Centro Carter, quienes estuvieron a cargo de la dirección general del proyecto.

Para la elaboración, redacción y edición de este informe contribuyeron numerosos autores, incluyendo Ingo Boltz, Marcelo Escolar, Avery Davis-Roberts, David Carroll, Jennifer McCoy, Héctor Vanolli, Raúl Sánchez Urribarrí y María Fernández.

Resumen ejecutivo

En respuesta a una invitación del Consejo Nacional Electoral de Venezuela (CNE), el Centro Carter organizó una misión técnica especializada para la observación del sistema de votación automatizado utilizado durante las elecciones presidenciales del 3 de diciembre de 2006. Los objetivos principales de la Misión fueron demostrar el apoyo de la comunidad internacional a la realización de elecciones democráticas en la República Bolivariana de Venezuela y contribuir con un proyecto más ambicioso del Centro Carter, tendiente a desarrollar y actualizar las metodologías para la observación y evaluación de sistemas de votación electrónica en el plano mundial.

Los observadores de la Misión del Centro Carter llegaron a Caracas el 22 de noviembre de 2006, luego de que se hubieren completado muchas de las auditorías pre-electorales. El equipo de la Misión tuvo sin embargo la posibilidad de observar, además de un cierto número de auditorías y pruebas en las dos semanas previas al día de la elección, la auditoría "en caliente" realizada el día de los comicios y la auditoría post-electoral. Dado el arribo tardío de la Misión al país, las observaciones directas del equipo del Centro Carter se complementaron con el análisis de las actas oficiales de aquellas auditorías que tuvieron lugar antes de su llegada, información recibida del CNE y entrevistas con representantes de partidos políticos y asociaciones civiles y personal del CNE y de la empresa Smartmatic. Los registros de observación más detallados, en especial los relacionados a las auditorías del código fuente y la actividad observada en el centro de tráfico de red, se incluyen en un capítulo anexo.

El presente documento se divide en cinco capítulos: 1) Diseño institucional y contexto político del proceso electoral; 2) Diseño y funcionamiento del sistema de votación automatizado venezolano; 3) Mecanismos de seguridad de las máquinas de votación; 4) Transmisión de resultados y 5) Plan de auditorías. En un capítulo adicional se incluyen las conclusiones y recomendaciones de la Misión.

Diseño institucional y contexto político del proceso electoral venezolano.

Atento al hecho de que la comprensión exhaustiva del marco legal e institucional en que se desarrolla la elección es un aspecto importante de la observación técnica, en este capítulo se reseña el diseño del Poder Electoral venezolano, la conformación del Consejo Nacional Electoral (CNE), el impacto de las nuevas tecnologías en la estructura del CNE y las medidas tomadas por el organismo electoral para incrementar la confianza ciudadana en el sistema de votación automatizado.

De acuerdo a lo establecido en la constitución y las leyes, la administración, ejecución y supervisión de todo lo concerniente a los asuntos electorales está a cargo de un quinto poder del estado, el poder electoral. Debido a esta circunstancia, el proceso electoral venezolano se encuentra dentro de la jurisdicción exclusiva de una autoridad estatal autónoma. Por un lado, esta circunstancia facilitó la adopción rápida y extendida de tecnologías electorales electrónicas. Por otro lado, en un contexto de alta polarización política, esa misma autonomía contribuyó a despertar preocupación entre los sectores de la oposición respecto de la integridad del sistema de votación automatizado, así como respecto a un supuesto partidismo por parte de los actuales rectores del CNE, por el hecho de que éstos fueron nombrados por una legislatura dominada por el oficialismo.

Venezuela utilizó tecnologías de votación electrónica por primera vez en una prueba piloto implementada

en las elecciones 1993 y, en mayor escala, en las elecciones 1998. Posteriormente, en las elecciones de 2004, se introdujeron las llamadas máquinas de votación electrónica directa (o DREs, por sus siglas en inglés, con pantallas sensibles al tacto) con la intención de establecer eventualmente un sistema de votación completamente automatizado, que incluyera la automatización de procesos tales como la identificación del votante, la emisión del voto, la transmisión y totalización de los resultados y la inscripción de los candidatos.

Durante las elecciones de 2006, en el marco de una amplia ronda de consultas con representantes de oposición, el CNE adoptó una serie de importantes medidas para fortalecer la confianza pública en el proceso electoral, incluyendo una serie de auditorias pre y post comiciales, una auditoría "en caliente" del 53 por ciento de mesas de votación, la desconexión de las máquinas de votación durante el día de las elecciones y la impresión del registro de los votos emitidos por cada máquina antes de la transmisión de los resultados.

El sistema de votación automatizado ha alcanzado un buen nivel del funcionamiento técnico. Para asegurar la confianza pública en el sistema, y evitar la necesidad de continuas negociaciones ad hoc, en este documento se sugiere transformar las citadas medidas en regulaciones estándar.

Diseño y funcionamiento del sistema de votación electrónica.

En este capítulo se examinan los diversos aspectos de las máquinas de votación Smartmatic que se utilizaron durante la elección presidencial de 2006, incluyendo tanto los aspectos relativos al funcionamiento de dichas máquinas durante el día de la elección como los aspectos vinculados la usabilidad y el diseño de las mismas.

La Misión del Centro Carter comprobó que las máquinas funcionaron correctamente, lo que permitió a los electores emitir su voto sin inconvenientes. Sin embargo, se observaron algunos detalles relacionados con el diseño, como la confusión que generó entre algunos votantes el cambio de paradigma entre elegir a un candidato tocando el tablero sensible al tacto y emitir un voto en blanco en la pantalla táctil. Otro aspecto observado fue la aparente falta de procedimientos dirigidos a que el elector corrija su voto, en caso que éste alegue que el comprobante de voto impreso no refleja su elección. Otros aspectos observados se relacionan a ciertas características de diseño, que podrían dificultar la emisión del voto a personas analfabetas, y al tiempo acordado por la máquina para la emisión del voto.

Mecanismos de seguridad de las máquinas de votación.

En esta sección se evalúan las medidas de seguridad técnicas y físicas que se implementaron en el sistema de votación electrónico en Venezuela. La Misión pudo apreciar que el CNE tomó recaudos razonables respecto de la seguridad de las máquinas, incluyendo la encriptación de la información sobre la votación almacenada en la memoria, el uso de mecanismos aleatorios para impedir la reconstrucción de la secuencia del voto y la seguridad referente a los comprobantes impresos en papel.

El CNE implementó además una serie de resguardos para promover la seguridad física de las máquinas, los que incluyeron medidas referentes a la cadena de custodia, a fin de que las máquinas no pudieran ser manipuladas maliciosamente. El equipo del Centro Carter observó varios incidentes menores, que sugieren cierta confusión entre las autoridades de mesa y los oficiales del Plan República en cuanto a los protocolos destinados a prevenir la manipulación maliciosa y la falta de normas claras y uniformes para todo el personal que participa en la elección. Si bien tales hechos no prueban que haya existido manipulación, sí demuestran que es teóricamente posible. Los futuros procesos electorales se verían por lo tanto beneficiados con una mayor claridad respecto de los procedimientos y la aplicación uniforme de los protocolos electorales.

Transmisión de resultados.

En este capítulo se analizan los medios de transmisión de los votos desde los centros de votación hasta el Centro de Tabulación Central (el Sistema Central de Totalización) así como las medidas de seguridad que se implementaron para proteger ese proceso y el sistema de tabulación.

El equipo del Centro Carter pudo comprobar que el CNE dio importantes pasos para proteger el sistema electrónico contra posibles ataques externos, que pudieran afectar la integridad de los votos almacenados en las máquinas y/o la transmisión de los votos desde la máquina de votación hasta el centro de totalización. A la misión le resultó sin embargo más difícil evaluar el grado de seguridad del sistema contra potenciales ataques internos (los que pueden ocurrir en cualquier sistema de votación electrónico), o el grado de seguridad en el sistema central de totalización. No obstante ello, el equipo del Centro Carter considera que el sistema se beneficiaría con el agregado de niveles de seguridad adicionales, que pudieran protegerlo de potenciales vulnerabilidades internas.

Plan de auditorías.

Venezuela implementó un gran número de auditorías durante los tres meses previos a la elección, el mismo día de la elección y en el período inmediatamente posterior a los comicios, entre las que se contaron auditorías del software y el hardware. Dada su amplitud y profundidad, puede concluirse que el plan de auditorias implementado para las elecciones de diciembre de 2006 tiene el potencial de convertirse en una herramienta analítica sólida para asegurar la integridad del proceso electoral.

Para alcanzar este objetivo, el Centro Carter considera que podrían tomarse diversas medidas tanto en la etapa precomicial como en las etapas comicial y post comicial. Esas medidas podrían incluir una comparación obligatoria del recuento de comprobantes impresos en papel con los resultados del voto electrónico durante el día de la auditoría "en caliente," la determinación previa de un margen de error y un nivel de confianza respecto de las muestras de auditoría con antelación a la misma, y permitir que el recuento de los comprobantes de voto constituyan la base para un cuestionamiento legal de los resultados de votación electrónica.

En la etapa pre-electoral, la aplicación de una serie de medidas destinadas a mejorar diversos aspectos procedimentales, podría contribuir sustancialmente al logro de los objetivos de la llamada auditoría "pre-despacho".

Conclusiones y recomendaciones.

En virtud de la magnitud y duración de su Misión de Observación Técnica Especializada, el Centro Carter, no está en condiciones de efectuar una evaluación exhaustiva del proceso electoral ni de la integridad del sistema electrónico de votación utilizado en Venezuela. Pese a ello, y teniendo en cuenta los aspectos del sistema electrónico de votación que la misión pudo observar y analizar, el Centro Carter brinda en esta sección una serie detallada de recomendaciones destinadas a fortalecer los diversos aspectos del proceso electoral vinculados al sistema de votación automatizada, que podrían ayudar a mejorar el desempeño del mismo en el futuro.

El Programa de Observación Técnica Especializada del Centro Carter

En respuesta a una invitación del Consejo Nacional Electoral de Venezuela, el Centro Carter organizó una misión técnica especializada para las elecciones presidenciales del 3 de diciembre de 2006. Según la Declaración de Principios para la Observación Internacional de Elecciones, firmada por más de 20 organizaciones internacionales en las Naciones Unidas en octubre de 2005, las misiones internacionales de observación pueden ser exhaustivas (cuando están destinadas a evaluar el proceso electoral en su totalidad) o especializadas (cuando se limitan a la observación de aspectos particulares del proceso).

En este caso en particular, la Misión Técnica del Centro Carter observó el uso de las tecnologías de votación automatizada en Venezuela. La misión tuvo dos objetivos principales: a) demostrar el apoyo de la comunidad internacional a la realización de elecciones democráticas en la República Bolivariana de Venezuela; y b) contribuir a un proyecto más ambicioso del Centro Carter, tendiente a desarrollar y actualizar metodologías para la observación y evaluación de sistemas de votación automatizados en el plano mundial.

Idealmente, los miembros de la Misión del Centro Carter deberían haber llegado a Venezuela con bastante antelación al día de la elección, a fin de observar la totalidad de las auditorías y pruebas pre-electorales auspiciadas por el CNE. Factores tales como la invitación tardía por parte del CNE (9 de octubre de 2006) y la necesidad de recolectar fondos impidieron que el Centro Carter pudiera organizar una misión con la debida antelación.

Dadas las circunstancias antes mencionadas, los observadores del Centro Carter arribaron al país una vez que muchas de las auditorías pre-electorales habían sido completadas, pudiendo solamente observar un número limitado de éstas durante las dos semanas anteriores al día de la elección. Debido a estos factores, las observaciones directas realizadas por los observadores del Centro Carter durante el periodo pre-electoral fueron complementadas con información recibida del CNE, del proveedor tecnológico (Smartmatic), y de los partidos políticos.

Dado el alcance focalizado de la Misión, el día de la elección los observadores del Centro Carter cumplieron su tarea en centros de votación seleccionados especialmente a fin de evaluar la influencia de factores sociales, culturales y ambientales en la usabilidad y funcionamiento de las máquinas de votación, así como en la implementación de los procedimientos de administración de la elección. Específicamente, se observó el impacto de los factores humanos (situación económica y nivel de educación de los electores, grado de polarización política y grado de participación política) y los diferentes métodos de transmisión de resultados (línea telefónica fija, celulares o traslado físico al centro de transmisión de contingencia) en el desarrollo de los acontecimientos en los centros de votación (ver Anexo I).

Debido a las limitaciones en materia de tiempo y recursos humanos, la Misión del Centro Carter no produjo una evaluación exhaustiva del proceso electoral en su totalidad ni de la integridad del sistema electrónico de votación utilizado en Venezuela. Este informe resume las observaciones de la misión con respecto al funcionamiento del sistema durante las elecciones presidenciales del 3 de diciembre de 2006 en base a un análisis comparativo de los sistemas usados en otras jurisdicciones, sugiriendo además una serie de recomendaciones.

Diseño Institucional y Contexto político del Proceso Electoral Venezolano

La observación de los componentes electrónicos del proceso electoral comprende, en sentido estricto, la evaluación de la seguridad, la usabilidad y el funcionamiento técnico del sistema y sus mecanismos. Para que esa observación sea completa se debe sin embargo tener también en cuenta el marco legal e institucional en el que tienen lugar las elecciones, así como la dinámica y las características del sistema político. Todos estos factores influyen en el nivel de confianza de la ciudadanía en el proceso electoral, lo que a su vez afecta la usabilidad y el funcionamiento técnico del sistema. Los procesos de polarización política, por ejemplo, impactan la forma en que el público percibe a las instituciones que garantizan la seguridad de los sistemas, las que además pueden verse afectadas por la falta de participación de los sectores de oposición en los procesos de toma de decisiones, asi como por la existencia de asimetrías en la información entre los actores políticos.[1]

Por todo ello, la observación de los componentes electrónicos del sistema electoral constituye apenas una parte del esfuerzo para evaluar la calidad general del proceso electoral.

El poder Electoral venezolano

El diseño del actual proceso electoral venezolano se encuentra regulado por la Constitución de la República Bolivariana de Venezuela, la Ley Orgánica del Poder Electoral, la Ley Orgánica de Sufragio y Participación Política,[2] la Ley de los Partidos Políticos, Reuniones Públicas y Manifestaciones y el Estatuto Electoral del Poder Público. Estas normas constitucionales y legales establecen un sistema institucional en cuyo centro se encuentra el Poder Electoral, el poder del estado al que se le confía la administración, ejecución y supervisión de todo lo concerniente a los asuntos electorales.[3]

Debido a esta circunstancia, el proceso electoral en Venezuela se encuentra dentro de la jurisdicción exclusiva de una autoridad estatal autónoma.[4] Para asegurar su independencia de los otros poderes del estado, la Constitución dotó al Poder Electoral de los principios de independencia orgánica, autonomía funcional y autonomía presupuestaria (art. 294). Así, desde el punto de vista presupuestario, le corresponde al propio Poder Electoral preparar su presupuesto a solicitud de su presidente. El Poder Ejecutivo sólo lo deriva, sin modificación alguna, a la Asamblea Nacional.

1 Se trata de una versión especial de la llamada "paradoja de la capacidad" (Hartlyn, McCoy, 2006: 47), entendida como el resultado de las características institucionales de los órganos electorales, el nivel de complejidad de los componentes electrónicos utilizados y el contexto de competencia política. En estas condiciones, las dudas de naturaleza tecnológica provocan asimetría, lo que hace difícil la observación, fomentando en los sectores de oposición la suposición de que el partido oficialista es "capaz" de cometer fraude mediante medios técnicos que no dan a conocer.

2 Gran parte de esta ley, que data de 1997, ha sido reformada por la Constitución de la República Bolivariana de Venezuela de 1999, y por la más reciente Ley Orgánica del Poder Electoral.

3 La reforma constitucional de 1999 le dio rango constitucional a los órganos de control electoral (art. 113), rango con el que no contaban en la Constitución de 1961 (en la que sólo tenían jerarquía legal).

4 Modelos institucionales similares en relación a este tipo de atribuciones podrían ser el Instituto Federal Electoral de México (IFE), la Corte Electoral de Bolivia y el Registro Civil Nacional de Colombia, aunque ninguno de estos tres casos emula al régimen electoral venezolano en cuanto a los niveles de poder y autonomía. En el caso de México, además del IFE existe el Tribunal Electoral del Poder Judicial de la Federación, que no sólo tiene a su cargo la resolución de conflictos surgidos en el marco de las contiendas electorales, sino también el conteo final y la proclamación de los candidatos que hayan sido elegidos. El IFE tiene jurisdicción similar a la del CNE respecto del registro electoral, pero no es responsable de la totalidad de la cadena de documentación ya que los registros civiles están fuera de su mandato en el plano administrativo y jerárquico. La Corte Electoral de Bolivia puede tener un parecido más estrecho con el Poder Electoral venezolano, si bien comparte algunas funciones con la Policía Nacional. En el caso de Colombia, la responsabilidad administrativa del proceso electoral recae en el Registro Civil, aunque éste está exento de las responsabilidades jurisdiccionales, las iniciativas legislativas, el recuento final de votos y la proclamación de los candidatos electos. Nicaragua posee también un cuarto poder de estado en el Consejo Supremo Electoral (CSE), que es responsable de administrar las elecciones, dar a conocer los resultados finales y resolver conflictos (sus decisiones son inapelables ante cualquier tribunal o poder del gobierno).

El Poder Electoral está asimismo regido por los principios de despartidización de los organismos electorales, imparcialidad y participación ciudadana, como así también de los principios de descentralización de la administración electoral, transparencia y celeridad del acto de votación y escrutinios (art. 294). Entre las principales atribuciones del Poder Electoral se encuentran:

- la facultad de introducir legislación electoral;
- el control de su presupuesto, sin intervención del poder ejecutivo;
- la facultad de tomar decisiones legalmente vinculantes en calidad de autoridad estatal;
- la atribución de contratar personal a través del Servicio Electoral; y
- el control de todas las etapas y procesos vinculados al proceso electoral, incluyendo el registro civil de las personas, el registro de los electorales; la regulación de las organizaciones políticas, las campañas proselitistas y el financiamiento; la proclamación de candidaturas electorales y el registro de afiliaciones políticas; los procedimientos del día de las elecciones (tales como la identificación de los electores y la emisión, totalización, transmisión, conteo y comunicación electoral de los votos); el anuncio y proclamación de los candidatos electos; el control administrativo y la supervisión general del proceso electoral, teniendo incluso la potestad de declarar la nulidad total o parcial de las elecciones.

El Poder Electoral regula además todos los asuntos electorales que no están contemplados por la constitución ni por las leyes pertinentes mediante decretos o reglamentaciones de su ente rector, el Consejo Nacional Electoral (CNE).

El Consejo Nacional Electoral (CNE)

Como se acaba de señalar, el Poder Electoral está conformado por el Consejo Nacional Electoral (CNE), que actúa como el organismo de gobierno en todo lo relativo a los asuntos electorales. El CNE, a su vez, está compuesto de cinco rectores, cuyos mandatos tienen una duración de siete años, además de un secretario (que es elegido por los rectores). El organismo es presidido por uno de los rectores, que se elige entre sus miembros en reunión plenaria. Cada rector tiene dos suplentes.

Los organismos bajo su dependencia son:

- La Junta Nacional Electoral (JNE). La JNE es un organismo colegiado con dos miembros titulares y un miembro suplente. Entre otras funciones, es responsable del planeamiento y ejecución de elecciones y referendos y puede presentar propuestas al CNE respecto de la administración de la elección;
- La Comisión de Registro Civil y Electoral (CRCE). La CRCE es un organismo colegiado administrativo de naturaleza descentralizada. Sus miembros incluyen a los directores de aquellos organismos que son responsables del proceso de registro civil y electoral, así como miembros principales y suplentes del CNE. A la CRCE se le confía la gestión administrativa de los registros civiles y de electores;
- La Comisión de Participación Política y Financiamiento. La Comisión de Participación Política y Financiamiento es un organismo colegiado administrativo de naturaleza descentralizada. Sus miembros incluyen a los directores de aquellos organismos que son responsables de promover la participación política y supervisar y financiar las organizaciones políticas, así como miembros principales y suplentes del CNE.

Además de estos organismos existen otros organismos dependientes, regionales y municipales, tales como las Oficinas Electorales Regionales y las Juntas Electorales Regionales, Municipales, Metropolitanas y Parroquiales.

Selección de los rectores

Para la selección de los rectores, la Constitución prevé la participación de tres instituciones:

- El Poder Ciudadano[5] que tiene la facultad de postular un rector;
- Las facultades de ciencias políticas y jurídicas de las universidades nacionales, que tienen la facultad de postular un rector; y
- Un organismo ad-hoc, denominado Comité de Postulaciones Electorales, que tiene la facultad de postular tres candidatos sobre la base de sus méritos.[6]

La Asamblea Nacional se encarga entonces de seleccionar, entre los candidatos postulados, los cinco rectores titulares y sus respectivos suplentes mediante el voto afirmativo de las dos terceras partes.

El requisito de contar con las dos terceras partes de los votos (o mayoría calificada) apunta a asegurar el máximo reconocimiento de los miembros del Poder Electoral por parte de la ciudadanía, como así también la representatividad del organismo.

El actual CNE

El CNE que tuvo a su cargo la realización de las elecciones presidenciales de 2006 es el primer CNE designado según procedimientos delineados en la Constitución de 1999. En años anteriores, los miembros del CNE fueron designados mediante procedimientos distintos a los previstos por la Constitución, lo que contribuyó a incrementar la percepción entre algunos sectores de la población de cierto partidismo. En el año 2000, por ejemplo, debido a la falta de una legislatura nacional, el "pequeño comité" de la Asamblea Constituyente (conocido como "el Congresillo") designó rectores provisorios, que tuvieron a su cargo la dirección de las mega-elecciones del año 2000. Posteriormente, unos meses antes del referendo revocatorio de 2004, la Asamblea Nacional no pudo alcanzar los dos tercios necesarios para designar a los candidatos a ocupar el cargo de rectores lo que generó una serie de presentaciones ante la Sala Constitucional del Tribunal Supremo, en las que se instó a la Asamblea a efectuar tales designaciones.[7] Finalmente, le correspondió al Tribunal Supremo de Justicia nombrar a los rectores.[8]

Si bien el actual CNE es el primer CNE nombrado de acuerdo a la normativa constitucional, el retiro de las fuerzas de la oposición del proceso electoral correspondiente a los comicios parlamentarios de diciembre de 2005, a sólo tres días de la realización de las elecciones, tuvo como consecuencia que la Asamblea Nacional que designó a los nuevos miembros del organismo electoral en 2006 quedara totalmente en manos de agrupaciones políticas aliadas del gobierno. Debido a esta circunstancia, algunos sectores de la sociedad venezolana tienden a percibir el directorio del CNE como un cuerpo dominado por personalidades afines al gobierno, lo que, a ojos de esos sectores, impacta negativamente el nivel de confianza pública.

La introducción de nuevas tecnologías

Venezuela utilizó un sistema automatizado de votación por primera vez en una serie de pruebas piloto en 1993 y, a nivel general, en las elecciones de 1998. Debido a lo estipulado en el artículo 154 de la Ley Orgánica del Sufragio y Participación Política, el interés en dicha tecnología aumentó progresivamente en los años siguientes.[9] La relativa ausencia de obstáculos burocráticos y políticos para la gestión administrativa del CNE (tales como restricciones presupuestarias o controles por parte de la Asamblea u organismos del estado especializados) facilitó la

5 El Poder Ciudadano (el cuarto poder del estado) esta constituido por el Consejo Moral Republicano, integrado por el Defensor del Pueblo, el Fiscal General y el Contralor General de la República.

6 El Comité está constituido por once diputados elegidos por la Asamblea, que luego postula diez personas provenientes de diferentes sectores de la sociedad civil. Conjuntamente, esas 21 personas postulan tres rectores, que son elegidos por el voto de una mayoría de dos tercios de la Asamblea Nacional.

7 Véase, entre otros, el caso "Hermann Escarrá y otros" del 04/08/2003.

8 Sentencia del 25/08/2003.

9 El artículo 154 de la Ley Orgánica del Sufragio y Participación Política de 1998 establece que el proceso de votación, escrutinio, totalización y adjudicación "será totalmente automatizado", relegando el sistema manual solamente a los casos en los que el sistema automatizado no pudiere ser implementado "por razones de transporte, seguridad, infraestructura de servicios", casos que deben ser expresamente determinados, y con la debida antelación, por el CNE.

pronta incorporación a amplia escala de nuevas tecnologías de información y comunicación, las cuales no sólo abarcaron la emisión del voto sino además la transmisión de los datos, la identificación del elector y el registro de candidatos. Ello tuvo por consecuencia la conformación de un sistema de votación sumamente sofisticado de buen nivel de rendimiento técnico.[10] No obstante ello, en la medida en que ese proceso contribuyó a ensanchar la brecha de información respecto al uso del sistema, el mismo ha generado también cierto nivel de incertidumbre entre los actores.[11]

La experiencia internacional indica que la incorporación de las nuevas tecnologías de información y comunicación debe hacerse en forma paralela a un amplio proceso de consulta a los actores políticos.

La transición al sistema automatizado no ha estado exenta de dificultades. Prueba de ello han sido los cambios efectuados entre 1998 y 2006 en los dispositivos utilizados para la emisión automática de los votos. La decisión inicial de usar un sistema de escaneo óptico de boletas en las elecciones de 1998, 1999 y 2000 fue seguida por la decisión de utilizar un sistema con registro y verificación electrónica directa con máquinas con pantallas sensibles al tacto en el referendo de 2004, para finalizar con el sistema de votación electrónica directa a través de medios automatizados en las elecciones legislativas de 2005. Adicionalmente, en el proceso revocatorio y en las elecciones regionales del 2004 se implementaron oficialmente procedimientos de identificación y registro biométricos mediante las llamadas "máquinas captahuellas," los que, en los procesos electorales recientes, pasaron a ser un complemento del proceso de identificación de electores.[12]

El modelo tecnológico adoptado por la República Bolivariana de Venezuela tiene por objetivo lograr la automatización de la totalidad de los procedimientos electorales (incluidos los procedimientos vinculados a la identificación de electores) en cumplimiento a lo dispuesto en la normativa constitucional y legal correspondiente.

El propósito normativo de estas disposiciones legales y constitucionales es el de mejorar el funcionamiento y la calidad de los procedimientos tradicionales, haciéndolos más seguros y confiables. La experiencia internacional indica sin embargo que la incorporación de las nuevas tecnologías de información y comunicación debe hacerse en forma paralela a un amplio proceso de consulta a los actores políticos. Sin este requisito, el proceso de automatización del sistema electoral puede tener resultados no queridos, tales como el aumento de las dudas sobre dicho proceso por parte de los sectores políticos que no participan en el proceso de toma de decisiones relativas a esas tecnologías.

Impacto de las nuevas tecnologías en la estructura burocrática administrativa

La incorporación continua de las nuevas tecnologías en las diferentes etapas del proceso electoral venezolano ha afectado la estructura burocrático-administrativa del CNE en varias maneras:

Aumento de la centralización de la gestión del proceso electoral. El proceso de automatización requiere, entre

10 En los casos de Brasil y Bélgica, el proceso fue más gradual. En otros casos, tal como el de México, Argentina y Australia, los órganos electorales se opusieron a la automatización acelerada (Instituto Federal Electoral de México, Cámara Nacional Electoral de Argentina y la Federal Electoral Office de Australia). La introducción de tecnologías adoptó por lo tanto la forma de pruebas de ensayo y error a nivel regional para desarrollar y estudiar el uso de otras tecnologías en situaciones de votación reales, en algunos casos con tecnología desarrollada por ellos mismos (Canberra 2002 y 2004, Buenos Aires 2005), en otros, con tecnología propietaria (Ciudad de México 2004, Ushuaia 2003).

11 En este punto resulta relevante la comparación con el caso de Brasil. Aunque la sofisticación técnica es menor que en Venezuela, en este país se alcanzó rápidamente consenso respecto de la solución técnica implementada, y los actores políticos y la sociedad civil están de acuerdo en que la automatización representa una mejora para el proceso electoral.

12 CNE, Resolución Nº 04811-1104 del 11, de agosto de 2004, y Resolución Nº 041022-1621, del 22 de octubre de 2004.

otras cosas, que las decisiones relacionadas con la información, organización y logística se concentren gradualmente en un centro de toma de decisiones que sea capaz de garantizar el manejo replicado, coordinado y unificado de los dispositivos y sistemas utilizados, así como también su seguridad. Esta circunstancia ha tendido a impactar directamente la estructura orgánica del CNE beneficiando las áreas tecnológicas mediante una mayor asignación de recursos. El rol del directorio del CNE y de sus subordinados directos—los encargados de las diferentes áreas ejecutivas de la organización—ha tendido de esa forma a fortalecerse.

El actual CNE ha dado importantes pasos para continuar, fortalecer y expandir el proceso de diálogo e intercambio entre el organismo electoral y los factores de la oposición

Aumento del nivel técnico promedio de los funcionarios públicos a cargo de las diferentes etapas del sistema y ensanche de la brecha de información y conocimiento entre las diferentes áreas administrativas. Las soluciones tecnológicas adoptadas por el CNE tienden a tornarse cada día más sofisticadas, así como a utilizarse en un mayor número de regiones del país. En consecuencia, el personal necesario para ocuparse del mantenimiento de estas soluciones durante los periodos no electorales, y para supervisar su funcionamiento durante el proceso electoral, tiende a aumentar, no solo en cuanto a la cantidad, sino también en cuanto al nivel de capacitación técnica que se requiere para cumplir esas funciones.

Los miembros del personal técnico cumplen además numerosas funciones en el proceso electoral. La concentración de responsabilidad dentro de este grupo tiende por lo tanto a reducir la autoridad del personal electoral tradicional dado que las decisiones se toman en estratos más elevados de la jerarquía electoral. En particular, esta circunstancia tiende a afectar a aquellos funcionarios responsables de las actividades de organización y logística tradicionales durante los procesos electorales, así como también al personal de nivel intermedio de los centros de votación y de los centros municipales y regionales del Poder Electoral.

Reducción de la gestión directa de los procesos electorales mediante la tercerización. Si bien la introducción de soluciones automatizadas tiende a provocar el crecimiento de las áreas tecnológicas de los organismos electorales, la necesidad de subcontratar empresas especializadas para la gestión de algunos de los aspectos del proceso electoral tiende a hacer dichos organismos dependientes, en mayor o menor medida, de los servicios de esas empresas. En el caso del CNE, la dependencia inicial con Smartmatic, la empresa proveedora de la tecnología de las máquinas de votación, se ha reducido progresivamente en años recientes, en la medida que el organismo electoral pasó a involucrarse en la totalidad de las áreas del proceso electoral ya sea asumiendo la gestión de las operaciones directamente (con apoyo de los técnicos de la empresa) o asumiendo un rol supervisor.

El organismo electoral, por ejemplo, ha asumido actualmente en forma íntegra la capacitación de los electores, los miembros de mesa y los operadores (que estuvo inicialmente en manos de Smartmatic). La empresa, por su parte, mantiene a su cargo la logística y la coordinación del despliegue de la plataforma de voto automatizado; la preparación y puesta a punto de la infraestructura tecnológica; el aprovisionamiento de los operadores; el soporte técnico a nivel nacional y la gerencia de proyectos y servicios de financiamiento del proyecto asociados a la elección. En cuanto a la plataforma tecnológica, Smartmatic suministró la infraestructura hasta el año 2004. Posteriormente, suministró equipamiento adicional para satisfacer demandas vinculadas al crecimiento del registro electoral. Actualmente, dado que el CNE ha adquirido toda su infraestructura tecnológ-

ica, y es propietario de la misma, el que suministra los equipos en cada elección es el propio organismo electoral.[13]

Gestión tecnologica, confianza y transparencia

La implementación exitosa de procesos electorales automatizados requiere el cumplimiento de ciertos pasos esenciales, que tengan como fin mitigar la desconfianza de los actores políticos e institucionales no involucrados en el proceso de toma de decisiones o la gestión o administración de las elecciones.

Los procesos electorales manuales se basan por lo general en procedimientos protocolares administrativos estándar, que deben cumplirse a medida que se desarrolla el cronograma electoral. A fin de construir confianza pública, estos procedimientos incluyen la llamada "cadena de custodia" del cotillón electoral y los registros de documentos utilizados para la identificación de los electores. La cadena de custodia y el control descentralizado del proceso electoral tienen además lugar en las mesas de votación durante la emisión y el conteo manual de votos, donde los ciudadanos pueden ver lo que está sucediendo.

En el caso de los sistemas automatizados, la necesidad de contar con sistemas de administración logística complejos—que por lo general están tercerizados—, hace difícil, en la práctica, el cumplimiento del principio de descentralización de los procesos de la cadena de custodia lo que, en algunos casos, puede despertar dudas sobre su transparencia. Por esa razón, los intentos tradicionales de construcción de confianza asociados al sistema manual deben complementarse, en los sistemas automatizados, con medidas específicas para las nuevas tecnologías.

Por consiguiente, a fin de aumentar la transparencia del proceso electoral, los sistemas de votación automatizados deben desarrollar mecanismos de auditorías técnicas apropiados. Para que esas auditorías cumplan realmente su función, las mismas deben contemplar, de manera exhaustiva, la totalidad de los componentes automatizados, así como basarse en un conocimiento completo y detallado de la arquitectura del sistema. Contra este escenario debe por lo tanto analizarse el plan de auditorías llevado a cabo por el CNE durante las elecciones de diciembre de 2006 (ver Capítulo 5).

Proceso de diálogo con la oposición

El actual CNE ha dado importantes pasos para continuar, fortalecer y expandir el proceso de diálogo e intercambio entre el organismo electoral y los factores de la oposición iniciado durante los procesos electorales posteriores al referendo revocatorio de 2004. El 29 de abril de 2006, el Directorio del organismo electoral convocó a la totalidad de los sectores políticos del país a fin de "asegurar las garantías y las condiciones electorales que permitan la participación de la ciudadanía el 3 de diciembre,"[14] dando oficialmente inicio al proceso de consultas y contactos el 10 de mayo (el plazo para recepción de solicitudes al CNE por parte de los partidos políticos se estableció hasta el 31 de julio).

De acuerdo a información suministrada por funcionarios del CNE, del citado proceso de dialogo participaron 17 precandidatos y 38 organizaciones políticas. Durante el transcurso del mismo fueron elevadas 55 propuestas y demandas, de las cuales, según la información oficial, el CNE aceptó y aprobó el 76 por ciento.

Entre las medidas más importantes tendientes a fortalecer el nivel de confianza pública en el proceso electoral, y facilitar la participación ciudadana, debe mencionarse la decisión de auditar, el mismo día de la elección, entre el 53 y el 55 por ciento de las

13 El CNE parece haber optado hasta el momento por adquirir lo que, a su parecer, tiene sentido económico y estratégico, subcontratando a Smartmatic, y a otros proveedores, para la mayoría de las necesidades que requieren de alta especialización, y que no constituyen necesidades cotidianas del CNE. De acuerdo a lo expresado al equipo del Centro Carter por un alto funcionario de la empresa, en muchos casos, para el CNE es económicamente más rentable contratar los servicios de Smartmatic una vez al año, cuando se los necesita, que construir una especie de "Smartmatic interno del CNE", lo que tendría altos costos y altos requerimientos gerenciales, pero que permanecería ociosa en los períodos no electorales.

14 Información oficial provista por el CNE.

mesas de votación mediante la llamada auditoria "en caliente" (ver Capítulo 5). Otra medida de similar impacto en la confianza pública fue la decisión de reiterar las medidas de seguridad relativas al proceso de transmisión pactadas en procesos electorales anteriores, tales como las de mantener las máquinas de votación desconectadas durante la jornada de votación (a fin de impedir cualquier transmisión no autorizada), e imprimir un acta con los votos emitidos en cada mesa antes de que la máquina inicie el proceso de transmisión de los resultados al centro de totalización.

En la misma ronda de consultas se acordó la realización de un proceso integral de auditorias a la plataforma de votación, con la participación de auditores de los partidos políticos y observadores nacionales e internacionales, así como la revisión de los protocolos de auditoria. Estas decisiones hicieron posible el ambicioso plan de auditoria efectuado al sistema de votación automatizado antes, durante y después de las elecciones de diciembre de 2006 (ver Capítulo 5).

Igualmente importante para la transparencia del proceso electoral fue la decisión del CNE de entregar a los representantes de los partidos políticos de oposición, una hora antes de la difusión del primer anuncio oficial de los resultados, un CD contentivo de la lista de todas las actas computadas hasta ese momento. Esa medida permitió a los partidos políticos participantes de la contienda electoral contrastar los resultados de los comicios mesa por mesa.

Todas estas medidas tuvieron un importante impacto en el proceso de fortalecimiento de la confianza pública. Las mismas, sin embargo, se pactaron de manera ad hoc para cada uno de los procesos electorales. La Misión del Centro Carter considera que el nivel de confianza pública se incrementaría aún más si la mayoría de estos acuerdos se incorporara a la normativa regular oficial del CNE, de forma de evitar la nueva discusión de las mismos en cada uno de los procesos electorales.

Resumen de recomendaciones

- Incorporar los procedimientos pactados en los últimos procesos electorales entre el CNE y los factores políticos a tanto a la normativa regular del organismo electoral como a los procedimientos estándares de operación.

Detalles técnicos del sistema de votación electrónica

Las máquinas Smartmatic son máquinas de votación electrónica directa (DRE, por su sigla en inglés). A diferencia de otras modalidades, que almacenan la información sobre el voto en medios pasibles de ser leídos automáticamente (tales como los sistemas de escaneo óptico, que leen boletas de papel), la máquinas de votación DRE capturan el voto directamente en una memoria electrónica. Debido a sus características, las máquinas de votación electrónica directa se están utilizando cada vez más en diversos lugares del mundo, tales como Australia, Bélgica, Brasil y varios estados de los Estados Unidos.

En las elecciones presidenciales 2006 en Venezuela se utilizaron dos modelos de máquinas de votación: la máquina Smartmatic SAES 3000 y la máquina Smartmatic SAES 3300 (ver Figura 1)

El modelo SAES 3000 es el modelo más antiguo. Basado originalmente en una estación terminal para loterías, el mismo fue fabricado por la empresa Olivetti para Smartmatic. Ha estado en uso durante varios años.

Smartmatic SAES 3000

Smartmatic SAES 3300

Figura 1: Máquinas de votación Smartmatic SAES 3000 y SAES 3300

El modelo SAES 3300 es el modelo más moderno. Fabricado en Taiwán en base a un diseño propio de Smartmatic, el mismo ofrece una serie de mejoras con respecto al modelo anterior. Entre otras características, la máquina SAES 3300 dispone de tecnología asistencial para discapacitados, capacidad de audio y teclas especiales para no videntes. En las elecciones del 2006, sin embargo, no se utilizó ninguno de los componentes que distinguen este modelo dado que el software necesario para incorporarlos no estuvo disponible a tiempo para las elecciones.[15] Así, el modelo 3300 operó con el mismo software de votación que el modelo 3000, quedando por lo tanto inutilizados sus componentes especiales.[16] Por esta razón, en el presente informe no se hacen distinciones entre los dos modelos.

El sistema operativo utilizado en ambas máquinas es el Windows XP Embedded. Ambos modelos operan con un software de votación creado específicamente para las elecciones venezolanas, escrito en el lenguaje de programación C#, que utiliza la plataforma Microsoft.NET.

Hardware

Los modelos SAES 3000 y SAES 3300 comparten los siguientes componentes clave:

- pantalla táctil color (la pantalla del modelo 3300 es algo más grande)
- impresora térmica integrada con cortador de papel
- memoria interna (sin disco rígido)
- puertos periféricos y de comunicación (un puerto Ethernet y un módem)

15 Entrevista con personal técnico del CNE

16 Ciertos detalles del sistema operativo, tal como los controladores de dispositivos, pueden variar de modelo a modelo dado que el hardware no es exactamente el mismo en ambas máquinas.

Figura 2: Botón de activación remota

- memoria extraíble para puerto USB incluida con puerto separado
- bloqueo físico para evitar que se abra la máquina

Componentes periféricos

Los dos modelos funcionan con el mismo conjunto de periféricos:

- Botón de activación remota, conectado a la máquina mediante un cable a uno de los puertos PS/2 de la máquina (ver Figura 2).
- Tablero sensible al tacto con las opciones de voto (que se conecta a uno de los puertos PS/2 de la máquina mediante un cable). Las opciones de voto están impresas en una boleta de papel, que se superpone a los botones sensibles al tacto del tablero. La boleta de papel indica el lugar en el que debe presionar el elector para pulsar la tecla que está por debajo. A diferencia de procesos electorales anteriores, en las que se usaron varios tableros conectados entre si, en las elecciones presidenciales de 2006, las opciones de voto se ordenaron en un único tablero (ver Figura 3).

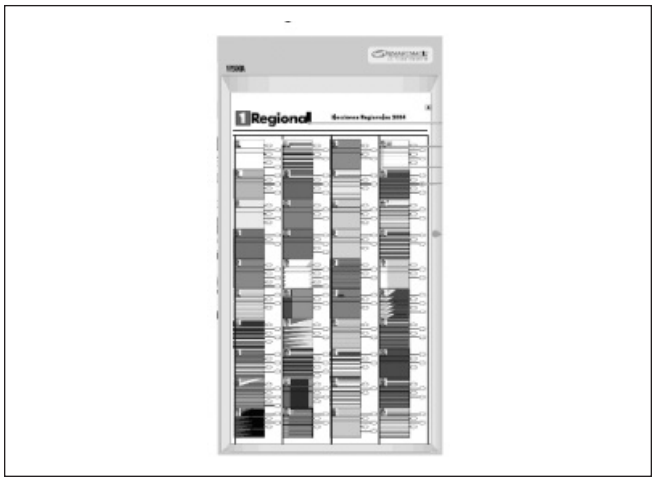


Figura 3: Tablero sensible al tacto con las opciones de voto

Descripción del funcionamiento del sistema el día de las elecciones

La descripción de los siguientes procedimientos se refiere a la parte del proceso electoral relacionada con el funcionamiento de las máquinas de votación y se divide en: a) apertura del centro de votación; b) votación y c) cierre del centro de votación.

Apertura del centro de votación:

Para proceder a la apertura de la votación, la normativa electoral establece los siguientes pasos:

- El operador verifica que las condiciones físicas para el funcionamiento de la máquina de votación estén en orden (provisión de electricidad, ubicación de las mamparas para resguardar la privacidad, etc.);
- Mediante la pantalla táctil, el operador introduce una contraseña (que es única para cada máquina), a fin de desbloquear la máquina de votación e ingresar al menú del operador;[17]
- El operador accede al menú y ejecuta los diagnósticos del sistema para verificar que todos los componentes funcionen de manera correcta. Imprime luego un reporte de diagnóstico (en caso de que se produzca una falla, sigue los procedimientos de contingencia);
- El operador inicia el proceso electoral, que comienza con la impresión de dos actas de inicialización en cero;
- El primer elector procede entonces a votar.

17 Este menú controla funciones ocultas al elector, tales como los diagnósticos, la apertura y cierre de la votación y la transmisión.

Votación

Durante la votación, las normas establecen los siguientes pasos:

Autorización de acceso.

Una vez que el elector se ha identificado, el presidente de mesa presiona el botón de activación remota ubicado en su escritorio, lo que permite desbloquear la máquina de votación durante tres minutos. Si el elector no emite su voto en ese lapso, la máquina se bloquea automáticamente. El presidente de mesa debe entonces volver a presionar el botón de activación remota para permitir que el elector cuente con tres minutos adicionales para votar. Una vez transcurridos estos tres minutos, no es posible desbloquear nuevamente la máquina.[18]

Presentación de las opciones de voto.

Una vez que la máquina ha sido desbloqueada, el elector repasa las opciones de voto disponibles en la boleta electoral, la cual está colocada sobre el tablero sensible al tacto de la máquina. Cada opción contiene una pequeña fotografía del candidato, su nombre y el partido al que pertenece.

Selección de las opciones de voto.

El elector presiona entonces un pequeño óvalo ubicado al lado del candidato de su preferencia, lo que activa el botón correspondiente del tablero sensible al tacto que se encuentra debajo de la boleta electoral. Una vez hecho esto, en la pantalla táctil aparece una imagen amplificada de la opción seleccionada por el elector, incluyendo el nombre del candidato, su fotografía y el nombre del partido. Si la imagen no coincide con el candidato seleccionado por el elector, éste tiene la posibilidad de presionar el botón correspondiente al candidato de su preferencia, hasta definir la opción deseada.

Dado que en el tablero sensible al tacto no existe un botón específico para el voto en blanco, el elector que desea ejercer esta opción tiene las siguientes posibilidades:

- No presionar ninguno de los botones correspondientes a los candidatos sobre el tablero sensible al tacto. En ese caso, la parte de la pantalla táctil donde debería aparecer la opción seleccionada por el elector permanece en blanco;
- Si el elector ya ha seleccionado un candidato y luego cambia de parecer, y decide emitir un voto en blanco, éste puede presionar la imagen del candidato seleccionado en la pantalla táctil. De este modo, la imagen desaparece, siendo reemplazada por un espacio en blanco.

Confirmación del voto.

Mientras visualiza la imagen correspondiente a la opción seleccionada en la mitad superior de la pantalla táctil (o un espacio en blanco en caso de haber optado por el voto en blanco), el elector presiona el botón "Votar", que se encuentra en la mitad inferior de dicha pantalla. En el caso de no haber seleccionado un candidato, la máquina le pide que confirme su elección ("¿Está seguro de que desea votar en blanco? Sí/No"). Si, por el contrario, seleccionó un candidato, el voto se confirma directamente mediante la presión del botón "Votar". La decisión no puede anularse.

Almacenamiento del voto.

Para casos de contingencia, cada voto se almacena electrónicamente en dos lugares distintos: la memoria interna de la máquina y la memoria extraíble conectada al puerto USB.

Comprobante de voto.

Luego de que el elector confirma su voto en la pantalla, y éste queda almacenado electrónicamente, la máquina imprime un comprobante en el que se visualiza el nombre del candidato seleccionado y el partido. A diferencia de la boleta electoral que se encuentra sobre el tablero de votación sensible al tacto, en el comprobante de voto no aparece la imagen del candidato. El presidente de mesa solicita entonces al elector que verifique su comprobante de voto, lo doble y lo deposite en una urna física.

18 Esta característica no es una limitación tecníca, impuesta por la máquina de votación, sino por las regulaciones del CNE.

No existen procedimientos que permitan cambiar el voto en los casos en que el elector afirme que el comprobante no refleja fielmente su voto. El voto electrónico no puede anularse una vez que ha sido confirmado en la pantalla y, conforme a los procedimientos establecidos para el funcionamiento de los centros de votación, el elector está obligado a depositar el comprobante de voto en la urna en todos los casos.

Resguardo mediante tinta indeleble.
Una vez que el comprobante de voto ha sido depositado en la urna, uno de los miembros de mesa entinta el dedo meñique del elector con tinta indeleble como medida de resguardo adicional para evitar que se vote más de una vez. Hecho esto, el elector se retira del centro de votación.

Cierre del centro de votación

Al finalizar la votación, las autoridades de mesa deben cerrar la mesa de votación y completar el proceso de votación. Para ello, se siguen los pasos descriptos a continuación:

- El operador de la máquina de votación introduce nuevamente la contraseña única para acceder al menú del operador;
- El operador presiona entonces el botón "Finalizar la votación" y confirma esta opción mediante la contraseña única. Una vez cerrada, la votación no puede reabrirse utilizando esa máquina;
- El operador imprime seis copias del acta de escrutinio (cuatro de las cuales se entregan a los testigos de los partidos políticos);
- El operador conecta la máquina a un medio de comunicación y transmite los resultados al servidor de totalización (si la transmisión desde el centro de votación falla, o si resulta imposible realizarla desde ese centro debido a la falta de conexiones fijas o móviles, se quita la memoria extraíble conteniendo una de las dos copias de la votación y se transporta al Centro de Transmisión de Contingencias-CTC más cercano, desde donde se efectúa la transmisión).
- El operador imprime un reporte detallado, no secuencial, de los votos emitidos por la máquina conocido como "chorizo", consistente en una copia de resguardo de cada uno de los comprobantes de voto impresos durante el acto electoral.[19] Las copias impresas son idénticas a los comprobantes de voto verificados por los electores durante la votación, por lo que básicamente constituyen una segunda versión del acta de escrutinio en forma de boletas de papel (de acuerdo a las autoridades electorales, el objetivo básico del "chorizo" es ayudar a los miembros de mesa a identificar cualquier comprobante de voto que no se encuentre en la urna durante la auditoria del día de la elección).[20]
- Las máquinas y los documentos se guardan en sus respectivos embalajes y se entregan a los efectivos militares para ser almacenados y transportados.

Otros procedimientos

Antes, durante y después del día de la votación se lleva a cabo una serie de procedimientos adicionales, tales como los procedimientos vinculados al establecimiento, funcionamiento y cierre de la mesa electoral y los procedimientos vinculados a la auditoria que se realiza el día de la elección (conocida como "auditoría en caliente"). Los mismos no se incluyen en este capítulo ya que el principal objetivo del mismo es ilustrar el funcionamiento de la máquina de votación y no el proceso electoral en su conjunto.

19 La impresión es no secuencial para evitar la reconstrucción de la secuencia de los votos.

20 La impresión de estas copias no se menciona como procedimiento estándar en el Manual para las Autoridades de Mesa, aunque sí se lo hace en el Manual para los Operadores.

Sistema Automático de Identificación de Huellas Dactilares

Antes de proceder a la votación, en cierto número de centros de votación, el elector debía proceder a identificarse mediante el llamado Sistema Automático de Identificación de Huellas Dactilares (AFIS)[21]. La descripción de este sistema no se incluye en este informe ya que el mismo no forma parte del sistema de votación automatizado. Su uso, además, no constituye un requisito legal para la emisión del voto.

Conclusiones sobre la usabilidad y diseño de las máquinas de votación

Durante la observación del sistema de votación automatizado, la Misión del Centro Carter pudo constatar que, en general, las máquinas de votación funcionaron correctamente, lo que permitió a los electores emitir su voto sin inconvenientes. A juicio de la Misión, podría sin embargo ser necesario reconsiderar algunos aspectos del diseño de las máquinas.

La utilización simultánea de la pantalla táctil y el tablero sensible al tacto puede haber confundido a algunos electores. Como se explicó anteriormente, al emitirse el voto, la máquina de votación determina que el lugar donde el elector selecciona su preferencia es el tablero mientras que el lugar donde el elector visualiza y confirma su voto es la pantalla. Sin embargo, si se emite un voto en blanco, la máquina cambia el patrón, ya que la pantalla pasa a ser tanto el lugar donde el elector selecciona su voto como el lugar donde lo confirma. El tablero, por lo tanto, no cumple en este caso ninguna función. El día de la elección, los observadores de la Misión fueron testigos de varios casos de confusión entre electores, que afirmaban no haber podido emitir un voto en blanco o haber votado en blanco por accidente, provocados posiblemente por esta circunstancia. Si bien el porcentaje de votos nulos fue ínfimo,[22] la Misión del Centro Carter sugiere que el CNE considere eliminar el cambio de paradigma del proceso de interfaz de usuario para el voto en blanco.

Como se mencionó anteriormente, para finalizar la emisión del voto, el elector debe retirar manualmente el comprobante de voto, verificar que éste refleje fielmente la opción seleccionada y depositarlo en la urna. La manipulación de los comprobantes de voto por parte de los electores puede sin embargo inducir la comisión de errores humanos tales como el hecho de que el elector se lleve consigo, accidental o intencionalmente, el comprobante de voto. Dada esta circunstancia, el CNE podría considerar la implementación de prácticas que eviten la manipulación del comprobante de voto (una de estas prácticas podría ser que el elector pueda ver el voto detrás de un vidrio sin necesidad de manipularlo).[23]

Adicionalmente, los observadores del Centro Carter notaron que no se prevé ningún procedimiento para los casos en los que el elector alegue que el comprobante de voto no coincide con el voto que apareció en pantalla. Esta circunstancia atenta contra el propósito que tiene la verificación del comprobante de voto. Si el elector alega que existe una discrepancia entre su intención de voto y el comprobante impreso, éste debería tener la posibilidad de anular su voto, y volver a votar. En este caso, se debería poder suprimir el voto electrónico e invalidar el comprobante ya sea mediante su destrucción física o mediante la impresión de la palabra “anulado” en el mismo.[24] En el diseño venezolano, el elector que alega tal discrepancia no puede anular su voto.

21 El AFIS se empleó sólo en unos pocos estados, y únicamente en centros de votación que excedían los 700 electores. El principal objetivo de su empleo fue agregar huellas digitales adicionales al registro central de electores para su futura utilización, y acelerar la orientación que se brinda a los electores en los centros de votación, informándoles en qué página del cuaderno de votación (legalmente obligatorio) figuraba su nombre.

22 De acuerdo a cifras provistas por el CNE, el porcentaje de votos nulos fue del 1,35 por ciento de la votación (lo que corresponde a 160.245 votos).

23 Tales diseños se incluyen en la máquina de votación Diebold AccuVote TSX con impresora AccuView; la máquina Diebold/Procomp con impresora, que fue utilizada en Brasil; y los prototipos REV y LOV utilizados durante el ensayo de votación electrónica en Buenos Aires en 2005. Ver Calvo, Escolar, Pomares (2007), Gobierno Ciudad Autónoma de Buenos Aires (2005).

24 Diebold AccuVote TSX y prototipos utilizados en Buenos Aires, ibid.

De acuerdo a lo observado por algunos de los miembros de la Misión del Centro Carter, durante la jornada electoral una electora de mediana edad afirmó que el comprobante de voto no coincidía con el voto que ella había emitido en la pantalla. Las autoridades del centro de votación le pidieron que igualmente depositara el comprobante, pero la electora rehusó hacerlo.Finalmente, en señal de protesta, rompió el papel, metió los pedazos en la urna y se retiró.

Otro de los inconvenientes observados es que el comprobante de voto, mediante el cual el elector confirma que la máquina haya capturado su voto correctamente, no contiene la imagen del candidato. Un elector analfabeto puede emitir su voto en la pantalla guiado por la imagen del candidato y los símbolos del partido. Sin embargo, no podría confirmar ese voto en el comprobante, dado que en el mismo no aparece ninguno de esos elementos.

Por ultimo, el límite de tiempo impuesto por la máquina de votación al elector puede plantear un serio dilema entre la exigencia de seguridad y el derecho al voto. Debido a su actual configuración, la máquina permite sólo tres minutos para votar antes de bloquearse (con una única extensión de tres minutos adicionales). Esta medida tiene por objetivo evitar el acceso a la máquina sin autorización en caso de que no haya nadie controlándola una vez que haya sido desbloqueada por el presidente de mesa. Esta circunstancia, sin embargo, limita de hecho la cantidad de intentos de voto a la que tendría derecho el elector.

Resumen de recomendaciones

- Eliminar el cambio de paradigma del proceso de la interfaz de usuario para el voto en blanco. El tablero sensible al tacto debería contar con un botón aparte para "voto en blanco". Y esa opción debería visualizarse, y confirmarse, en la pantalla táctil, tal como se hace en el caso de los votos comunes;
- Modificar el diseño de la emisión del comprobante de voto para minimizar la manipulación de los comprobantes. A fin de evitar que los electores se lleven involuntariamente los comprobantes de voto del centro de votación, se podría considerar modificar el diseño de la emisión del comprobante de voto;
- Permitir que los electores tengan la posibilidad de cancelar su voto si el comprobante no refleja fielmente su elección;
- Incluir fotografías de los candidatos y símbolos de los partidos en el comprobante de voto. Esta media permitiría que los electores analfabetos confirmen su voto sin que nadie tenga que ayudarlos;
- Reconsiderar el criterio de otorgar dos períodos de tres minutos para votar. El derecho al voto no debería ponerse en peligro por dificultades inherentes al manejo del software de las máquinas de votación por parte de los electores.

Mecanismos de seguridad de las máquinas de votación

El diseño de las máquinas de votación Smartmatic presenta una importante serie de mecanismos de seguridad. Los principales son los siguientes:

- Encriptación (cifrado) de la información sobre los votos almacenada en la memoria interna/ memoria extraíble;
- Mecanismos de randomización para impedir la reconstrucción de la secuencia de voto;
- Mecanismo de "enlace" de la memoria extraíble con la máquina de votación a la que se conecta durante la inicialización, lo que impide que este dispositivo pueda ser cambiado por otro;
- Deshabilitación de cualquier puerto que no sea necesario para la operación estándar durante el día de la votación y remoción de sus controladores del sistema operativo;
- Seguridad del comprobante de voto.
- Cadenade custodia de las máquinas de votación.

Adicionalmente, durante las elecciones de diciembre de 2006 se implementó una serie de medidas para reforzar tanto la seguridad física de las máquinas (utilización de precintos de seguridad en las cajas conteniendo las máquinas y, en algunos casos, en los puertos) como la llamada cadena de custodia.

Encriptación (cifrado) de la información sobre los votos

Cada uno de los votos emitidos en las máquinas de votación se almacena como un archivo encriptado y separado en el sistema NTFS, tanto de la memoria interna como de la memoria extraíble. La encriptación que se utiliza es un algoritmo simétrico (AES 256-bit), cuya contraseña se genera al azar durante la instalación del software, siendo ésta única para cada máquina. Conforme a la documentación provista por el CNE y la empresa Smartmatic, la "semilla de generación" de la contraseña es una contraseña maestra, cuya clave es compartida, en partes iguales, por el CNE y los representantes de los partidos políticos.[25]

En opinión de la Misión del Centro Carter, la decisión de usar algoritmos estándar de encriptación, tal como el AES-256, en lugar de recurrir a software propietario, es acertada. Tal decisión aumenta la transparencia y la seguridad general del sistema. Debe sin embargo tenerse en cuenta que el generador aleatorio utilizado para crear contraseñas para las máquinas tiene también importancia.[26]

Para que la contraseña de cada máquina de votación sea auténticamente aleatoria, la semilla que se introduce en el algoritmo que genera dicha contraseña debería ser diferente todas las veces aleatoria para cada contraseña que se crea. Las semillas de generación utilizadas en estos casos incluyen por lo general la hora en que aparece en la computadora o una combinación de variables ambientales, tales como la temperatura del disco rígido y de la CPU al momento de generar dicha contraseña. Los observadores del equipo del Centro Carter no pudieron constatar el uso de estas semillas en la generación de las contraseñas. Si, en lugar de ello, se hubieran utilizado semillas no aleatorias de manera constante, la seguridad de la solución se habría reducido considerablemente.

25 Smartmatic, "Smartmatic Automated Election Systems —SAES_v3.2 101006.pdf" (2006) página 9.

26 Dado que no fue posible obtener información sobre esta práctica en Venezuela, en este informe sólo se hace un análisis teórico.

Mecanismo de randomización para impedir reconstrucción de secuencia

A fin de evitar la reconstrucción de la secuencia de los votos (ya sea mediante las propiedades del archivo original o mediante su ubicación en el lugar de almacenamiento), el sistema prevé los siguientes pasos:[27]

- Cada voto se guarda utilizando un nombre de archivo generado al azar. La marca de fecha/hora se reemplaza por un valor estándar idéntico para todos los archivos de votación (fecha de la elección, hora de inicio de la máquina);
- Cada vez que se emite un voto se crea y guarda una cantidad aleatoria de archivos ficticios vacíos. El archivo que efectivamente contiene el voto se guarda con el nombre de esos archivos vacíos, después de lo cual estos últimos se borran;
- El espacio (variable) que queda después de la supresión de los archivos ficticios es ocupado por los siguientes archivos ficticios y el siguiente archivo de voto.
- Dado que la cantidad de archivos ficticios es aleatoria, no hay manera de predecir ni reconstruir la ubicación del siguiente archivo de voto en el disco rígido (por ejemplo, si se generan menos archivos ficticios, tanto estos archivos como el segundo archivo de voto pueden guardarse en algún lugar antes del primer archivo de voto; si—por el contrario- se crean más archivos ficticios, el segundo archivo de voto puede guardarse en algún lugar después del primer archivo de voto, y así sucesivamente).

En el período previo a las elecciones de diciembre de 2005, durante el transcurso de una de las auditorías realizadas a las máquinas de votación, se descubrió una posible forma de reconstruir la secuencia de voto utilizando los registros almacenados en la tabla maestra de archivos del sistema NTFS (MFT, por su sigla en inglés). Para evitar dicha reconstrucción, se agregó una medida adicional al proceso de randomización. Así, en distintos momentos a lo largo del día de la elección, se cambia dos veces el nombre de cada carpeta del sistema de archivos, lo que hace desaparecer las rutas de acceso que quedan en la MFT. Al finalizar la votación, todos los registros MFT del sistema muestran horas de acceso cercanas a la hora de cierre de la mesa, lo que hace imposible restaurar la secuencia. En opinión de la Misión del Centro Carter, este método para impedir la reconstrucción de la secuencia del voto es completo y seguro. La Misión del Centro Carter no tiene conocimiento de ningún otro sistema de votación electrónica (incluidos los utilizados en Brasil, Bélgica, Australia [Canberra] o India) en los que se haya hecho tanto hincapié en la posible reconstrucción de la secuencia de votación a través del análisis del sistema de archivos del disco rígido.[28]

Mecanismo de "Enlace" de la memoria extraíble con la maquina

De acuerdo al director del Departamento de Informática del CNE, la memoria extraíble en blanco se "enlaza" con la máquina en la que se instala, lo que hace imposible cambiarla por otra. Según la empresa Smartmatic, cuando una memoria extraíble se inserta por primera vez en una máquina, ésta transmite a la máquina una contraseña exclusiva.[29] De allí en adelante, se encriptan los votos tanto en la memoria interna de la máquina como en la memoria extraíble utilizando un algoritmo de encriptación AES-256bit y la contraseña exclusiva.

27 CNE (2006a)

28 Hay trabajos que analizan otros métodos de reconstrucción de la identidad del elector, tal como el de Brunazo (2004) en el caso de Brasil.

29 Presentación técnica de Smartmatic.

Según los procedimientos de contingencia documentados por el CNE, en los casos en que es necesario reemplazar una memoria extraíble o una máquina con fallas, ambas se "re-sincronizan", copiándose los votos registrados hasta ese momento en la unidad de reemplazo respectiva de modo que se duplica la base completa de datos. Una vez hecho esto, se utiliza la contraseña original para encriptar el resto de los votos registrados. Según el proveedor, la encriptación de la transmisión de la contraseña original en la unidad de reemplazo, mediante el uso de una contraseña especial idéntica para todas las máquinas y memorias extraíbles, resguarda adecuadamente este proceso de re-sincronización.[30]

Dado su impacto en la seguridad del sistema, resultaría útil contar con mayores detalles acerca de las medidas de seguridad respecto de esta "contraseña maestra." De revelarse la contraseña maestra, ésta podría permitir la creación de nuevas "memorias extraíbles en blanco." Al ser insertada en cualquier máquina de votación, la memoria extraíble podría autenticarse a sí misma utilizando esa contraseña maestra para simular una sincronización de contingencia y tener acceso a la contraseña exclusiva de cada máquina y a los votos almacenados en su memoria. La información de la que dispone la Misión del Centro Carter no es clara en cuanto a si se han implementado medidas de seguridad adicionales para evitar este posible tipo de manipulación

Deshabilitación de puertos no necesarios

La principal medida para evitar el acceso físico al interior de la máquina de votación es una cerradura con llave, que evita que se pueda abrirse el chasis. En ambos modelos, en el interior del chasis se encuentran el interruptor de encendido/apagado y el puerto USB que se usa para conectar la memoria extraíble. En algunas máquinas del modelo 3300, la misión observo que el puerto USB de la memoria extraíble estaba precintado además con una etiqueta de seguridad especial. En forma independiente al mecanismo de cierre, ambos modelos presentan además una serie de puertos (Serial, PS/2, Módem, Ethernet), a los que se puede acceder fácilmente, ya sea que cuenten con una cubierta de plástico (como en el caso del modelo 3000) o que no cuenten con ella (como en el caso del modelo 3300).

Según el proveedor, los puertos que no se necesitan se pueden deshabilitar de dos maneras: físicamente (evitando conectar los cables de los puertos correspondientes a los conectores de la placa madre); o mediante la aplicación de software, deshabilitando los puertos a través de Windows XP.

La Misión del Centro Carter no dispuso de información respecto de cuáles fueron los puertos que se deshabilitaron en las máquinas, por lo que no está en condiciones de efectuar un análisis más minucioso de la posibilidad de que se produzcan ataques locales a través de los mismos.[31]

Para impedir el acceso físico a las máquinas de votación, durante las elecciones de diciembre de 2006 se utilizaron, además de las cerraduras con llave, las llamadas "etiquetas de seguridad." De acuerdo a lo constatado por la Misión, si estas etiquetas se usan en forma permanente, se controlan exhaustivamente y se estipulan consecuencias de cumplimiento obligatorio en casos de violación, pueden efectivamente dificultar el acceso físico a la máquina o sus puertos, sirviendo así como elemento de disuasión.

30 Los dispositivos de contingencia sólo pueden sincronizarse con cualquier otro componente si la contraseña es reconocida por las memorias extraíbles y las máquinas.

31 Existe una diferencia significativa entre ambos mecanismos. La conexión física de los cables es un proceso que requiere invariablemente una intervención manual, máquina por máquina. Por ende, no es probable que en un ataque a la seguridad a gran escala se utilice este método. Por el contrario, la re-habilitación de los puertos deshabilitados mediante la utilización de software es mucho más fácil y, en teoría, podría lograrse utilizando software malintencionado, introducido centralmente por alguna persona bien informada implicada en el proceso. Un puerto deshabilitado mediante software es por lo tanto mucho más peligroso para el sistema de seguridad que uno deshabilitado físicamente.

El día de las elecciones, la Misión del Centro Carter observó que los puertos USB de varias máquinas contaban efectivamente con etiquetas de seguridad. Los procedimientos de seguridad en lo que respecta a esas etiquetas, sin embargo, parecían ambiguos. En el manual para los operadores de las máquinas distribuido por el CNE, por ejemplo, no se menciona la etiqueta cuando se describe el proceso de "verificación de la presencia de la memoria extraíble."[32] Tampoco se establecen consecuencias en caso se descubran intentos de quitar la etiqueta, ni instrucciones para volver a cubrir el puerto USB una vez verificada la presencia de la memoria.

Los observadores del Centro Carter notaron además diferencias en el modo en que los operadores manejaron el procedimiento relativo a las etiquetas de seguridad. En algunos casos, cuando se constataba que la etiqueta estaba rota, los operadores precintaron nuevamente el puerto con una nueva etiqueta. En otros casos, volvieron a "pegar" el precinto roto. En otros casos, el puerto quedó sin precintar. No quedó claro si los operadores conocían los procedimientos que debían seguirse en caso de ruptura de la etiqueta, o si consideraban la integridad de esa etiqueta como un elemento importante. En opinión de la Misión, el hecho de que no siempre se utilicen precintos de seguridad podría dejar a las máquinas vulnerables a violaciones a través de los puertos no precintados.

Con respecto a la llave del chasis, cabe notar que la misma es una llave genérica, lo que significa que todas las máquinas pueden abrirse con la misma llave. Se trata básicamente de una llave tubular simple, sin mecanismos de seguridad especiales. Dadas estas características, la Misión considera que, adicionalmente al uso de las etiquetas de seguridad, la utilización de una llave única para cada máquina, no genérica, podría mejorar la seguridad general de las mismas. Con 33.000 máquinas en funcionamiento que usan la misma llave, no resultaría difícil conseguir una llave de esas características, particularmente si se tiene en cuenta que ese tipo de llave puede adquirirse libremente en el mercado.[33]

Seguridad del comprobante de voto

Los comprobantes de voto (las boletas de papel que registran el voto, de forma que éste pueda ser verificado por el elector antes de ser depositado en la urna) contienen un importante número de medidas contra posibles falsificaciones. Entre otros elementos, los comprobantes de voto incorporan un sello de agua y están impresos con tinta de seguridad en un papel especial identificado con el logotipo del Poder Electoral.[34] Los comprobantes de voto incluyen, además, un número de serie exclusivo alfanumérico de 32 caracteres generados al azar, creado e impreso en tiempo real cuando se emite el voto. Dado que las variables que sirven de base para el algoritmo generador aleatorio son tanto específicas para cada máquina (código de su ubicación geográfica el día de la elección) como aleatorias (una combinación de las temperaturas de los distintos componentes de la computadora al momento de generar el código), cada máquina de votación produce un rango único de números de serie. La Misión del Centro Carter asume que el número de serie contiene mecanismos confiables tal como sumas de control para evitar la falsificación.[35]

Si bien el número de serie puede impedir la falsificación de los comprobantes de voto, su valor práctico real es limitado ya que no existe posibilidad de que tal número sea leido automáticamente. En consecuencia, si fuera necesario verificar la autenticidad de una gran

32 CNE (2006b)

33 Este punto débil de los mecanismos de cierre también se ha observado con frecuencia en otros países. En consecuencia, el sistema utilizado en Venezuela comparte este punto débil con gran cantidad de sistemas de todo el mundo.

34 No se pudieron determinar detalles sobre la composición de la "tinta de seguridad".

35 La documentación disponible no incluye detalles específicos.

cantidad de comprobantes de voto utilizando el referido código, el único método posible sería la lectura manual del mismo, así como la introducción de cada uno de los códigos al sistema. Esta falencia podría remediarse mediante la inclusión en el comprobante de voto de un código de barras, que pueda ser leído automáticamente por la máquina, además del número de serie.[36]

En resumen, aunque resulte matemáticamente imposible falsificar un código de seguridad, si fuera necesario realizar una verificación de la autenticidad de los comprobantes de voto a gran escala, la lectura manual de los códigos requeriría una gran cantidad de recursos humanos, así como un prolongado lapso de tiempo, lo que disminuiría su valor como medida de seguridad efectiva.[37]

…si los procedimientos de precintado de las cajas conteniendo las máquinas de votación se realizan en forma exhaustiva, la manipulación de las máquinas durante el traslado de las mismas debería resultar sumamente difícil.

Cadena de custodia de las máquinas de votación

Teniendo en cuenta la relativa facilidad de acceso a la máquina, gran parte de la responsabilidad por la seguridad física de las máquinas depende de la cadena de custodia. La cadena de custodia tiene por objetivo evitar el acceso no autorizado a las máquinas de votación durante el almacenamiento y traslado de las mismas. En Venezuela, este procedimiento depende principalmente de:

- una unidad especial de efectivos militares en actividad, llamada Plan República, creada específicamente para las elecciones y teóricamente bajo el control directo del CNE (y no del alto mando militar); y
- la cinta de seguridad con la que se precintan las cajas que contienen las máquinas de votación durante su traslado.

Los miembros del Plan República están a cargo de la custodia del local central donde se configuran las máquinas y se instala el software para la votación, así como también del transporte de las máquinas a los centros de votación de todo el país.[38]

De acuerdo a lo estipulado en la actual normativa, antes del traslado a los centros de votación respectivos, las cajas que contienen las máquinas de votación se precintan con una "cinta de seguridad" provista por el CNE. Al llegar a los centros de votación (lo que ocurre generalmente tres o cuatro días antes del día de la elección), las cajas con las máquinas de votación no deben abrirse sino quedar precintadas y almacenadas hasta el día de la instalación de los centros de votación (en el caso de las elecciones de diciembre de 2006, hasta el día viernes 1 de dicho mes). Ese día, las cajas deben abrirse en presencia de las autoridades de los centros de votación, los técnicos a cargo de las máquinas y los miembros del Plan República, de modo que pueda verificarse que las máquinas cuenten con la totalidad de los componentes y funcionen correctamente (diagnósticos de funcionamiento). Si no se detecta ningún problema, las cajas deben precintarse nuevamente con cinta de seguridad, la que debe ser firmada nuevamente por los miembros de mesa.

36 Smartmatic afirma que su sistema es capaz de producir tal código de barras, pero que el CNE no lo solicitó.

37 Una vez aclarado este punto, cabe señalar que hay poco material disponible que indique que en otros sistemas de votación electrónica se ponga tanto énfasis en mecanismos para evitar la falsificación de los comprobantes (en caso de que se utilicen). De allí que esta medida adicional, aunque no tenga mucha utilidad, no resta valor a la seguridad de los comprobantes de voto en Venezuela en el *benchmarking* internacional.

38 La logística y los medios de transporte (camiones, etc.) fueron provistos por AEROCAV, una empresa privada contratada por Smartmatic.

El día de la elección, las cajas deben abrirse en presencia de las autoridades de mesa y los testigos de los partidos para instalar y poner en funcionamiento las máquinas de votación. Una vez finalizada la elección, las máquinas deben colocarse nuevamente en las cajas, las que deben volver a precintarse con cinta de seguridad. Las autoridades de mesa deben firmar la nueva cinta de seguridad. Las cajas precintadas, con las máquinas en su interior, deben entonces enviarse de regreso al local central de logística para su posterior auditoría y almacenamiento.

Si los efectivos militares a cargo de la custodia de las máquinas cumplen su tarea de acuerdo a lo prescripto en las normas electorales, y los procedimientos de precintado de las cajas conteniendo las máquinas de votación se realizan en forma exhaustiva, la manipulación de las máquinas durante el traslado de las mismas debería resultar sumamente difícil.

Este proceso podría sin embargo fortalecerse mediante una mayor claridad respecto de los procedimientos establecidos y un aumento de la supervisión. Por ejemplo, ni el manual para las autoridades de los centros de votación[39] ni el manual para el Plan República[40] contienen instrucciones acerca del modo de verificar la integridad de la cinta de seguridad en el momento de la recepción de las máquinas el día de la instalación de los centros de votación (cuando las cajas llegan del local central y se abren por primera vez) o acerca de la configuración de las máquinas el día de la elección.[41] Únicamente el manual abreviado para los operadores de las máquinas contiene instrucciones sobre la verificación de la cinta en ambas ocasiones.[42] No obstante, la única respuesta allí definida, en caso de violación, es "llamar al centro de soporte técnico." La práctica comúnmente aceptada indica que todas las partes involucradas deberían compartir la responsabilidad por los procedimientos de la cadena de custodia/seguridad.[43]

Durante el cierre de la votación, los observadores de la Misión del Centro Carter notaron que en varios casos hubo confusión entre las autoridades de mesa respecto de los procedimientos a seguir para el precintado de las cajas contentivas del material electoral y los equipos. Entre otras cosas, se observó lo siguiente:

- Al precintar las cajas conteniendo el material electoral, algunas autoridades de mesa firmaron el cartón de las cajas en lugar de los bordes de la cinta de seguridad. Dado que había gran cantidad de cinta de seguridad en los centros de votación, y que no había nadie en particular que la custodiara, la mejor manera de evitar que alguien quitara la cinta, manipulara el contenido de las cajas y volviera a precintarlas con una nueva cinta era que las autoridades de mesa firmaran sobre el borde de la cinta original (falsificar firmas es sin duda más difícil que reemplazar cintas). En los casos en que sólo se firmaron las cajas, y no las cintas, el procedimiento de seguridad no funcionó como tal;
- Hubo autoridades de mesa que no pegaron las cintas de seguridad en las partes de las cajas que podían ser abiertas, sino en los costados. Dado que, en esos casos, no era necesario romper el precinto para abrir las cajas, una "caja precintada" podría haber sido manipulada sin que nadie se diera cuenta.

Si bien estos hechos no prueban que haya existido manipulación, sí demuestran que es teóricamente posible. Para solucionar este problema, en futuras elecciones debería mejorarse el mecanismo de cierre de las máquinas y los procedimientos de la cadena

39 CNE (2006c).

40 CNE (2006d).

41 Ambos manuales sí contienen instrucciones para el precintado de las cajas después del simulacro de votación o el cierre de las elecciones.

42 CNE (2006e).

43 Para mayor información, véase más adelante la sección en la que se resume la observación realizada por la Misión del Centro Carter del proceso de instalación de los centros.

de custodia. Estos hechos ponen de relieve la importancia que tiene la aplicación uniforme de las medidas de seguridad de la cadena de custodia.

Como corolario, puede afirmarse que la conveniencia de depender del sector militar para la custodia de las máquinas es dudosa. Dado que los militares están bajo el mando del poder ejecutivo, no son necesariamente imparciales. Aunque los efectivos militares del Plan República están en teoría bajo el control directo del CNE durante las elecciones, la Misión del Centro Carter observó varios casos en que los oficiales superiores hicieron caso omiso de las instrucciones del CNE, haciendo valer la tradicional cadena de mando.[44] Aun si el CNE tuviera control absoluto, el hecho de que algunos sectores consideren que éste está dominado por sectores afines al gobierno hace deseable que la sociedad civil, y especialmente la oposición, tengan una mayor participación en la custodia de las máquinas.

Resumen de recomendaciones

- Posibilitav que el número de serie de la boleta electoral pueda ser leído automáticamente por la máquina. De este modo, el número de serie se convierte en un mecanismo de seguridad funcional, que puede verificarse durante un recuento de boletas sin demasiado esfuerzo.
- Aclarar los procedimientos de seguridad física y exigir su aplicación uniforme. Estas medidas permitirían que las autoridades de mesa, los funcionarios electorales, los operadores de las máquinas y los efectivos militares del Plan República garanticen de manera más fácil la seguridad física de las máquinas, y harían que la utilización de precintos de seguridad cobrara mayor sentido como procedimiento de seguridad.
- Mejorar los procedimientos de la cadena de custodia relativos al traslado y almacenamiento de las máquinas. Esta medida podría incluir extender la responsabilidad respecto de la seguridad de las máquinas, durante los procesos de instalación y almacenamiento, a los partidos políticos y asociaciones civiles.

44 En un caso, un oficial superior prohibió a un oficial subalterno seguir el procedimiento del CNE y acompañar al presidente de mesa y los testigos a un Centro de Transmisión de Contingencia (CTC) después de que fallara la transmisión normal desde el centro de votación. Incluso se hizo caso omiso de llamadas provenientes de altas autoridades del CNE, que confirmaron que el procedimiento era el correcto e impartieron instrucciones al oficial subalterno para que hiciera lo que le habían solicitado las autoridades de mesa.

Transmisión de los resultados

De acuerdo a los procedimientos establecidos por el CNE, una vez finalizada la votación, y cerrada la mesa de votación, los votos almacenados durante la jornada electoral debían transmitirse electrónicamente al servidor central de totalización.[45]

Para la transmisión de los resultados se utilizaron los siguientes canales de transmisión:

Red de telefonía fija. La red de telefonía fija fue el medio estándar de transmisión en la mayoría de los centros de votación. Según la normativa aprobada por las autoridades electorales, una vez finalizada la votación, debía conectarse una línea telefónica al puerto RJ-45 del módem de la máquina de votación. La máquina debía entonces discar el número que la conectaba con un servidor de acceso remoto (RAS, por sus siglas en inglés), previa validación de la línea (contra la llamada "lista blanca")[46] y previa autenticación de la máquina contra un servidor AAA (autenticación, autorización y registro, según sus siglas en inglés). Una vez establecida la conexión, la máquina debía iniciar la transmisión a través del servidor de totalización en el CNE (el "servidor de recepción"). Si la recepción fallaba realizados dos intentos se debía dar por finalizado el intento de transmisión (se visualizaba en ese momento un mensaje de error). Los operadores de las máquinas de votación podían repetir el procedimiento todas las veces que lo consideraran necesario. Si no se lograba la transmisión, se debía pasar a la transmisión por telefonía celular y, de fallar ésta también, se debía pasar al traslado manual de la memoria extraíble a un Centro de Transmisión de Contingencia (CTC).

Telefonía celular. La telefonía celular fue el medio estándar de transmisión de *contingencia* utilizado en los casos en que falló la transmisión mediante telefonía fija. En algunos lugares de votación, donde no se disponía de línea telefónica fija, la transmisión por telefonía celular fue el único medio previsto. Para esta modalidad, se utilizó un teléfono celular provisto por el CNE a los operadores de las máquinas de votación. El procedimiento aprobado para esta circunstancia establecía que, luego de conectar el celular a la máquina de votación mediante un cable serial, debía procederse al discado, conexión y transmisión de los datos, de manera similar al procedimiento establecido para la transmisión mediante telefonía fija.

Telefonía satelital. La telefonía satelital debía utilizarse en los CTC ubicados en regiones donde no existía otro medio de transmisión posible.[47] En los CTCs de la mayoría de las zonas urbanas se utilizó la telefonía fija.

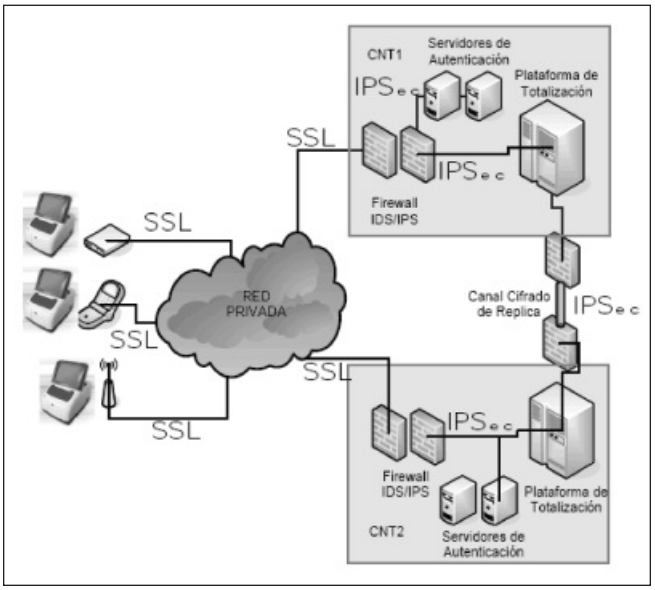


Figura 4: Topografía de la infraestructura de transmisión. Fuente: CNE, "SAES_v3.2 101006.pdf," 2006

45 La transmisión incluía tanto una lista agregada de los resultados de la votación (acta de escrutinio) como cada archivo de voto individual almacenado en la memoria interna y en la memoria extraíble.

46 Para mayor información sobre la "lista blanca", véase la siguiente sección en este mismo capítulo

47 Dado que el AFIS utilizaba transmisión satelital como medio estándar de comunicación con el cuaderno de votación electrónico (con el objeto de almacenar huellas digitales), en los lugares de votación en los que se instaló este sistema había antenas satelitales. Las redes, sin embargo, no estaban relacionadas ni interconectadas de manera alguna. La Misión del Centro Carter no pudo corroborar la utilización de los satélites. El Jefe Adjunto del departamento de informática del organismo electoral señaló verbalmente a un representante del Centro Carter que éstos no se habían usado durante las elecciones de diciembre de 2006.

La infraestructura de la red fue provista por CANTV, la compañía de telecomunicaciones de Venezuela, específicamente para este sistema electoral. La topografía de dicha infraestructura se describe a continuación:

Medidas de seguridad para la transmisión

Para el resguardo del proceso de transmisión de los resultados, el organismo electoral estableció los siguientes niveles de seguridad:

- *Infraestructura dedicada — Red privada (parcialmente virtual).* Sólo las líneas telefónicas enumeradas en una "lista blanca" podían discar el número previamente establecido para conectarse a los servidores RAS y acceder a la red privada. La lista blanca contenía el detalle de las líneas de telefonía fija instaladas en los centros de votación y los CTCs, así como también los teléfonos celulares distribuidos especialmente a los operadores de las máquinas y los técnicos.[48] Las líneas de telefonía fija y los teléfonos celulares no podían enviar ni recibir llamadas realizadas desde el sistema de telefonía pública.

  El día previo a las elecciones se eliminaron de la lista blanca los "candidatos dudosos", tales como los teléfonos celulares de los operadores de máquinas que no se presentaron a trabajar.[49] Asimismo, se creó una lista de "módems satelitales" aprobados para las conexiones satelitales. Sólo los módems aceptados podían comunicarse con la red.

  La transmisión de los resultados entre los servidores regionales RAS y los servidores centrales del CNE (denominados "CNT1" y "CNT2") viajó por una Red Privada Virtual (túneles seguros que usan IPsec). La misma arquitectura IPsec se usó para conectar:

  – el CNT1 del CNE con su servidor de contingencia CNT2;

  – internamente, los servidores de aplicaciones del CNE (servidores de recepción de datos y de consulta) con los servidores de la base de datos;

  – las autoridades electorales regionales (Juntas Regionales) con el CNT (funcionaron como CTC regionales).

- *Restricciones para consultas de los servidores de aplicaciones del CNE.* Los servidores de la base de datos sólo permitieron consultas de los servidores de aplicaciones del CNE (restricción basada en una dirección IP enlazada a una dirección MAC)

- *Autenticación RADIUS/AAA para todas las conexiones Dial-up y CDMA.* Las máquinas de votación cuyas líneas telefónicas figuraban en la "lista blanca" debieron además identificarse con un nombre de usuario/contraseña en un servidor RADIUS/AAA.

- *Comunicación encriptada (SSLv3/TLSv1) con autenticación recíproca.* Para la transmisión de los datos se utilizó una certificación creada por el CNE y Smartmatic el día de las elecciones, firmada digitalmente por la Autoridad de Certificación (AC) del CNE/Smartmatic. El contenido del paquete también se firmó digitalmente. Este esquema se utilizó tanto para la transmisión entre las máquinas de votación y el CNT como para la interfaz *Web* usada para consultar en tiempo real la base de datos con los resultados durante el día de las elecciones.

- *Protección de "cortafuegos" del CNT1 y 2* (con capacidad SPI/IDS/IPS).

- *Ubicación centralizada de los recursos físicos de computación del CNE.* Los recursos físicos de computación del CNE se centralizaron en una sola área, con acceso físico restringido. Se impuso igualmente acceso restringido a la administración de servidores, interruptores, cortafuegos, etc. (códigos de acceso compartidos entre el proveedor y el CNE).

48 El Centro Carter no pudo establecer si las líneas telefónicas fijas fueron instaladas especialmente por CANTV para las elecciones o si se utilizaron líneas telefónicas ya existentes (en general, las líneas telefónicas dedicadas se consideran más seguras).

49 De acuerdo a información provista verbalmente por funcionarios del CNE, con el objeto de purgar la "lista blanca", un día antes de la elección se realizó una auditoria, específicamente diseñada para ese propósito.

Medidas adicionales

Adicionalmente, para las elecciones de diciembre de 2006 se implementaron una serie de medidas adicionales de seguridad, la mayoría de las cuales fueron consensuadas con los sectores de oposición en los meses previos al acto comicial (ver Capítulo 1). Entre otras, pueden mencionarse las siguientes:

- las máquinas de votación no podían estar conectadas a ningún medio de comunicación durante el día de las elecciones (para evitar cualquier posible influencia a distancia sobre las máquinas);
- una vez cerrada la votación, por lo menos una de las actas de escrutinio generadas por la máquina de votación debía imprimirse antes de que se conectara la máquina para la transmisión de los resultados (para evitar que se realizaran cambios a distancia en la máquina durante la transmisión de los resultados); y
- los servidores AAA del CNE debían desactivarse hasta que la Junta Nacional Electoral (JNE) autorizara el inicio de la recepción. Hasta ese momento no se asignaban direcciones IP a las máquinas de votación y no se aceptaba la transmisión de los votos.

… para las elecciones de diciembre de 2006 se implementaron una serie de medidas adicionales de seguridad, la mayoría de las cuales fueron consensuadas con los sectores de oposición …

Un análisis detallado de posibles ataques a la infraestructura de la transmisión superaría el alcance de este informe. Sobre la base de la información disponible, puede sin embargo concluirse que la infraestructura de transmisión parece estar razonablemente bien protegida contra intrusiones externas.

La confianza de la ciudadanía en el sistema de votación electrónico podría sin embargo fortalecerse mediante decisiones tales como la de recurrir un proveedor de certificación externo independiente, en quien todas las partes confíen. La decisión de asignar ese rol a la Autoridad de Certificación del CNE puede incrementar innecesariamente la desconfianza, sobre todo en situaciones de extrema polarización política.

Funcionamiento del sistema central de totalizacion

De acuerdo a la normativa establecida para las elecciones de diciembre de 2006, luego del cierre de la votación, los votos almacenados en las máquinas de votación se debían transmitir al sistema central de totalización del CNE mediante el uso de la infraestructura de comunicaciones descrita anteriormente.

El sistema central de totalización estuvo compuesto de cuatro módulos principales (ver cuadro 1):

Configuración de la elección (EMS, por su sigla en inglés)

El EMS tuvo a su cargo recibir los datos electorales (tales como las opciones presentes en las boletas electorales y la información sobre el lugar de votación) y generar los archivos de configuración para cada máquina de votación. También generó la contraseña única para encriptar los archivos de votación y la contraseña necesaria para activar cada máquina de votación y acceder al menú del operador.

Configuración de la elección (EMS)
Cambio de alianzas (PEM)
Receptor de actas
Consulta de resultados (REIS)

Cuadro 1: Módulos del sistema de totalización. Fuente: CNE,SAES_v3.2 101006.pdf

Cambio de alianzas (PEM, por su sigla en inglés)

El PEM se utilizó para gestionar los cambios en las alianzas que realizan los candidatos, lo cual es sumamente corriente en la política venezolana. Los partidos políticos que inicialmente respaldaron a un determinado candidato para la presidencia pueden cambiar de aliados y apoyar a otro candidato durante el período previo a las elecciones. Y estos cambios pueden hacerlos hasta poco tiempo antes de las elecciones, incluso luego de que se hubieren impreso las boletas de papel que se colocan sobre los tableros sensibles al tacto, y ya no quede tiempo para volver a imprimirlas a fin de reflejar el cambio de apoyo a un candidato.

En consecuencia, durante las elecciones presidenciales de 2006, el papel colocado sobre los tableros sensibles al tacto, y la confirmación en la pantalla, no reflejaron ninguno de los cambios de último momento con respecto al respaldo a un candidato. Por lo tanto, es posible que haya aparecido en pantalla un voto a favor del partido A, que le diera un voto a favor al candidato presidencial B, cuando en realidad el partido A había pasado a respaldar al candidato presidencial C. Un elector desinformado, podría por lo tanto haber supuesto que estaba votando por el candidato B al votar a favor del partido A, cuando en realidad le estaba dando su voto al candidato C.[50]

Dadas sus implicancias, esta circunstancia constituye un punto débil importante de la usabilidad del sistema, por lo que el CNE debería considerar posibles soluciones a este problema. Una posible alternativa sería la de no permitir cambios en las alianzas una vez que se haya impreso la boleta electoral ya que, aún cuando los cambios de último momento en las alianzas partidarias pudiesen implementarse *en la pantalla*, las discrepancias entre ésta última y el tablero electoral sensible al tacto generarían confusión entre los electores.[51]

Dado que los cambios en el respaldo a un candidato no pueden manejarse localmente, los mismos se centralizan en el PEM. Las autoridades electorales locales introducen los cambios en el PEM mediante una interfaz *Web*,[52] que necesitan ser certificados por la Junta Nacional Electoral (JNE) antes de activarse. Si se aprueban, el módulo PEM asegura que los votos a favor del partido respectivo se contabilicen a favor del candidato al que recientemente se respaldó y no del anterior. Contar con detalles técnicos de dicho proceso de certificación y detalles de las políticas de seguridad que regulan el acceso a este módulo sensible permitiría realizar un análisis más minucioso de la seguridad del sistema PEM.

Receptor de actas

El receptor de actas es un servidor de aplicaciones cuya función fue la de recibir las transmisiones de los archivos de votación que llegaban tanto de las máquinas de votación como de las autoridades electorales locales (quienes transcribían los resultados manuales de los lugares de votación y los transmitían al CNE).

Las funciones del receptor de actas fueron las de:

- verificar la certificación del cliente que presentó cada máquina de votación;
- recibir los paquetes transmitidos (conteniendo los resultados de la votación);
- validar la integridad de los paquetes; y
- conectarse al servidor de la base de datos y escribir los resultados en la base.

El receptor de actas sólo recibe, verifica y pasa los resultados individuales transmitidos; no agrega información sobre la votación.

50 Esta circunstancia obliga a los electores a mantenerse informados sobre tales cambios, ya sea través de los medios de comunicación o del sitio *Web* del CNE, de forma que puedan tener en cuenta la información incorrecta que aparece en los tableros de votación sensibles al tacto. Sin embargo, teniendo en cuenta la gran cantidad de partidos políticos pequeños que existe en Venezuela, muchos de los cuales son generalmente poco conocidos, los cambios de respaldo a un candidato pueden pasar inadvertidos.

51 Como se explicó anteriormente, la interfaz de usuario de la máquina que aparece en pantalla repite la opción seleccionada en el tablero sensible al tacto.

52 Comunicación encriptada SSL 2048-bit

Consulta de resultados (REIS, por sus siglas en inglés)

El REIS tuvo por objetivo brindar acceso a información electoral en tiempo real a medida que se desarrollaba la votación el día de las elecciones. Esa información incluyó:

- información sobre la cantidad de máquinas de votación que ya habían realizado la transmisión;
- una visualización de los archivos de votos individuales transmitidos; e
- información sobre los resultados provisorios.[53]

El REIS se utilizó además para la emisión de boletines y otros documentos oficiales. El acceso al REIS está protegido por un nombre de usuario/contraseña con control de derechos de acceso. Se puede limitar el acceso de los usuarios permitiéndoles ver solo la información a la que están autorizados.

Acceso de autoridades locales

Las autoridades locales de los distintos estados tuvieron acceso al sistema central de totalización. El acceso conferido a dichas autoridades tuvo un doble objetivo:

- permitir el seguimiento del desarrollo de las actividades electorales durante la jornada electoral (base de datos de consulta de resultados);[54] y
- enviar los resultados de los centros de votación que utilizaron voto manual (dos por ciento del total) al CNT (se conectaron vía SSL al Receptor de actas, de manera similar a como lo haría una máquina de votación).

Medidas de seguridad del sistema central de totalización

Además de las restricciones respecto al acceso físico al edificio y los espacios en los que estuvo ubicado el sistema central de totalización, el esquema de seguridad establecido para el proceso de transmisión de los datos incluyó las siguientes medidas:

- protección de las aplicaciones que requieren la intervención del usuario mediante un nombre de usuario/contraseña con control de derechos de acceso;
- registro de la actividad de los usuarios y el sistema en todos los módulos; y
- almacenamiento de cada paquete que recibe el receptor de actas, a los fines de registro, en una base de datos local del servidor de aplicaciones que ejecuta el receptor de actas.

La eficacia de los esquemas de seguridad de acceso a todos estos módulos centrales tiene mucha importancia. Una persona con acceso al módulo PEM, por ejemplo, podría cambiar el respaldo de un candidato a otro, cambio que no podría ser observado por los electores o las autoridades de mesa debido a que no aparece en las máquinas. Dado que los partidos pequeños no atraen, por lo general, la atención del público, esos cambios podrían pasar desapercibidos.

Pese a la importancia de las medidas de seguridad, la cantidad de información detallada disponible sobre

53 Según la empresa Smartmatic "la máquina SAES facilita la impresión de documentos de conteo a medida que se tabulan los resultados" (2006a). No bien se produce cualquier acta de escrutinio, parcial o total, "estas actas pueden publicarse directamente en una página *Web* y ser vistas por el público." No quedó claro sin embargo hasta qué punto el CNE hizo uso de estas posibilidades durante las elecciones.

54 No quedó claro si esto incluye la posibilidad de ver los resultados agregados mientras los votos todavía están ingresando.

los procedimientos que resguardan el sistema central de totalización fue mucho menor que la cantidad de información disponible tanto sobre la seguridad de las máquinas de votación como sobre la seguridad de la transmisión. A los fines de juzgar la medidas de seguridad relativas al acceso a las herramientas de gestión del sistema, hubiera resultado de utilidad contar con mayor información sobre aspectos tales como la asignación de las combinaciones de nombre de usuario/contraseña a los usuarios; el establecimiento de los derechos de acceso (quién lo otorga, dónde y cómo se hace); el monitoreo de los registros de actividad del sistema (cómo se hace); y las políticas de respuesta—si las hubiera—, en caso de detectarse una anomalía. Sin información detallada sobre estos aspectos es difícil juzgar las medidas de seguridad implementadas.

Análisis general de la seguridad del sistema de transmision

El sistema utilizado en Venezuela es de carácter monolítico, no modular, tanto en los aspectos físico y lógico como en lo relativo al código fuente.[55] Debido a esta característica, el sistema debe ser protegido y auditado en su totalidad. Se trata básicamente de un sistema complejo, que cuenta con aproximadamente 200.000 líneas de código fuente[56] y un sistema operativo Microsoft Windows XP Embedded con muchas posibilidades de ser manipulado. Para contrarrestar esta amenaza se necesita un esquema de seguridad muy completo.[57]

Tal como se describió anteriormente, la encriptación y las firmas digitales tienen por objetivo proteger el almacenamiento de votos en la máquina y su transmisión al CNE. Dada la complejidad del sistema, y el hecho de que la Misión del Centro Carter no cuenta con las especificaciones necesarias a nivel de ingeniería ni con los detalles del código fuente, no es posible intentar aquí un análisis completo de la seguridad del sistema. Cabe sin embargo acotar que ningún sistema es cien por ciento seguro, y que existen sistemas que han demostrando ser más vulnerables a ataques que el de Smartmatic.[58]

En el caso específico de Venezuela, puede decirse que se han realizado esfuerzos razonables para proteger el sistema contra los ataques de intrusos tanto en lo que hace a la integridad de los votos (una vez que han sido almacenados en la máquina de votación) como en lo que hace a la transmisión de los mismos desde la máquina de votación al centro de totalización. Por el contrario, resulta difícil evaluar el nivel de seguridad en el sistema central de totalización. Puede afirmarse sin embargo que el sistema se beneficiaría con el agregado de niveles de seguridad adicionales, que pudieran protegerlo contra posibles ataques internos malintencionados. Una medida de esa índole podría incluir el uso de una autoridad de certificación externa, independiente y reconocida para emitir certificaciones que certifiquen la integridad de la comunicación entre las máquinas de votación y el centro de totalización

55 El modelo con tarjeta magnética utilizado en Bélgica, y el modelo conceptual "FROG" desarrollado por CalTech/MIT (2001), adoptan por ejemplo un enfoque modular. En ese enfoque, el primer módulo presenta las opciones de voto al elector y luego registra su elección en un medio que el elector puede verificar independientemente. Una vez que el elector verifica que su voto se ha registrado correctamente, introduce el medio en un segundo módulo. Ese modulo lee el medio y transmite (o almacena localmente) la selección allí registrada. Debido a que el elector verifica el voto registrado después de que el primer modulo completa su trabajo, el software de ese módulo no necesita ser protegido exhaustivamente. Unicamente el segundo módulo (que lee y transmite el voto almacenado de una manera que no es transparente para el elector) necesita estar muy bien protegido contra manipulaciones. Este segundo modulo es mucho más fácil de auditar porque contiene un código fuente más simple dado que la mayor parte de la lógica de presentación del sistema y la interfaz de votación del usuario (que requieren un código extenso) están localizados en el primer módulo. Por lo tanto, los sistemas modulares son mucho más fáciles de proteger que los sistemas monolíticos.

56 Cantidad estimada por un técnico de Smartmatic durante una entrevista.

57 El reemplazo de la tecnología de escaneo óptico (utilizada hasta 1998) por la tecnología de votación electrónica directa que se utiliza actualmente ha aumentado significativamente la necesidad de implementar medidas de seguridad, dado que los escáneres son un ejemplo de sistema modular.

58 Considérese, por ejemplo, las versiones iniciales del sistema Diebold AccuVote TS System, cuyos puntos débiles fueron expuestos por RABA (2004). Véase Tadayoshi, Stubblefield, Rubin, Wallach (2003)

Resumen de recomendaciones

- Considerar el uso de una Autoridad de Certificación independiente para emitir las certificaciones que protegen las comunicaciones entre las máquinas de votación y el centro de totalización. Esta medida de seguridad adicional ayudaría a proteger el sistema central de totalización contra posibles ataques;
- Aumentar la participación de los partidos políticos y los observadores en el proceso de auditoria, permitiéndoles realizar una observación formal del sistema central de totalización, incluidas las herramientas cruciales como el PEM. Esto aumentaría la transparencia y ayudaría a establecer mecanismos de seguridad de controles y equilibrios;
- No permitir los cambios de último momento en las alianzas partidarias. Ello evitaria la introducción de cambios en el PEM, que no se reflejen en el tablero.

Plan de auditorías

Para las elecciones presidenciales de 2006, el CNE implementó un plan de auditorías, que incluyó, entre otros procedimientos, auditorias pre-comiciales; una auditoria "en caliente" durante el día de los comicios y auditorias post-comiciales. Un importante rasgo de estas auditorias fue la participación de los representantes de las agrupaciones políticas inscriptas en la contienda electoral, quienes aprobaron formal y explícitamente, y en la totalidad de los casos, los procedimientos realizados. Dada su amplitud y profundidad, puede afirmarse que el esquema de auditorias implementado en Venezuela para las elecciones de diciembre de 2006 tiene el potencial de convertirse en una herramienta analítica sólida para asegurar la integridad del proceso electoral.

Dada su amplitud y profundidad, puede afirmarse que el esquema de auditorias tiene el potencial de convertirse en una herramienta analítica sólida para asegurar la integridad del proceso electoral.

Restricciones inherentes a los procesos de auditoría

A modo de introducción, es importante observar que los procesos de auditoría son, en esencia, imperfectos. La auditoría del código fuente, por ejemplo, considerada una de las auditorias más importantes del proceso electoral, tiene con frecuencia una eficacia limitada. Los expertos en software a cargo del examen del código fuente deben analizar un código que no ha sido creado por ellos, compuestos por gran cantidad de líneas de código. El sistema de votación electrónica AccuVote TS creado por Diebold, por ejemplo, contiene aproximadamente 285.000 líneas de código fuente,[59] mientras que el sistema Procomp, creado también por Diebold y utilizado en Brasil, tiene tres millones de líneas de código fuente.[60] Encontrar errores en tales cantidades equivale a buscar una aguja en un pajar. Por otra parte, un programador malintencionado intentaría en todos los casos ocultar las manipulaciones, por lo que resultaría aún más difícil descubrirlas.

Debido a estas dificultades, algunos expertos sostienen que los auditores no están en condiciones de asegurar, bajo ninguna circunstancia, que el software auditado sea cien por ciento seguro.[61] En cualquier auditoria de software es probable que haya errores que pasan inadvertidos. Y si hubo manipulaciones del código fuente, es muy posible que no se detecten.

A pesar de esta circunstancia, es importante recalcar que el diseño e implementación de un esquema integral de auditorías, conforme a las mejores prácticas, puede reducir ostensiblemente las posibilidades de errores y/o manipulación.

Para la evaluación de la seguridad de cualquier sistema de votación electrónica se recomiendan por lo general tres grandes pasos:

- un análisis documentado y especificado tanto del diseño técnico del sistema de votación electrónica como de las medidas de seguridad previstas, a fin de

59 RABA (2004).

60 Rezende (2004).

61 El experto en seguridad de sistemas de computación Ken Thompson (1984), por ejemplo, dice: "No se puede confiar en un código que uno no ha creado en su totalidad... Ninguna verificación o examen a nivel del código fuente brindan protección contra el uso de un código fuente que no es confiable… Un bug de micro código bien instalado es prácticamente imposible de detectar." Otros expertos, como Neumann (1993, 1995) y Mercuri (2002) concuerdan con esa opinión.

identificar y evaluar los posibles puntos débiles del sistema (y la posibilidad de manipulación en base a esos puntos débiles);

- una inspección minuciosa del sistema efectivamente en uso (incluido el software y el hardware), a fin de determinar si la tecnología que se utiliza durante el proceso electoral se ajusta a las especificaciones; y
- una inspección igualmente exhaustiva de los procedimientos no técnicos que se llevan a cabo antes, durante y después de las elecciones, a fin de determinar si las medidas que se tomaron cumplieron estrictamente con las normas y reglamentos estipulados.

Idealmente, el análisis del diseño técnico, y el detalle de las mejoras sugeridas para minimizar los riesgos identificados, deberían conducir a la implementación de mecanismos de seguridad adicionales, tanto técnicos (encriptación, firmas digitales, etc.) como no técnicos (precintos de seguridad, cerraduras, procedimientos claros en la cadena de custodia, políticas de acceso de personal, etc.), que tiendan a minimizar el riesgo de manipulaciones del sistema.

Si después de este proceso se llega a la conclusión de que el sistema es razonablemente seguro, y si tras la observación práctica se llega además a la conclusión de que el sistema auditado ha sido el mismo sistema utilizado durante los comicios, se podría afirmar, con cierta certidumbre, que el proceso electoral fue razonablemente seguro.

El esquema de auditorías utilizado en Venezuela

El plan de auditorías implementado en las elecciones presidenciales de 2006 en Venezuela comprendió una combinación de auditorías técnicas y no técnicas. Dado que el equipo de observadores del Centro Carter llegó el 22 de noviembre, algunas de estas auditorías ya se habían llevado a cabo, por lo que no pudieron ser observadas. Para remediar esta circunstancia, las Misión del Centro Carter intentó reconstruir parcialmente tales auditorias utilizando tanto copias de las actas oficiales de tales procedimientos[62] como entrevistas informales con los participantes de dichas auditorías.

Los bloques principales del plan de auditorías fueron los siguientes:

- Auditoria del hardware (máquinas de votación)
- Auditoria del código fuente (tanto en las máquinas de votación como en el sistema central de totalización)
- Auditoria de la infraestructura de transmisión
- Auditoria de "producción de las máquinas" y Auditoría "pre-despacho"
- Auditoria "en caliente" (día de la elección)
- Auditoría post electoral

Ademas de estas auditorias, el personal técnico del CNE llevó a cabo una serie de auditorías del software y el hardware del Sistema Automático de Identificación de Huellas Dactilares (AFIS). Dado que el AFIS no forma parte de este análisis técnico, y que la Misión del Centro Carter no estuvo presente durante esas auditorías, las mismas no se tienen en cuenta en el presente informe.

Asimismo, en los días previos a la votación se procedió a auditar los componentes no técnicos del sistema de votación, tales como los cuadernos de votación utilizados para identificar a los electores el día de la votación y el padrón electoral central utilizado para generar esos cuadernos. Dado que los mencionados componentes sólo están relacionadas de manera indirecta con el sistema de voto electrónico, y dado el hecho de que la Misión del Centro Carter no estuvo presente cuando se llevaron a cabo, tales auditorías tampoco se contemplan en este informe.

Por último, el proveedor efectuó también varias pruebas del sistema, algunas de ellas a gran escala, a fin de garantizar el funcionamiento del mismo. El

62 CNE (2006f)

presente informe tampoco se ocupará de estos ensayos debido a que no formaron parte del plan de auditorías públicas y no fueron observadas por la Misión del Centro Carter.

Cambios de procedimiento sobre la marcha

Una característica importante del proceso de auditorías fue su flexibilidad. Muchos de los detalles del proceso fueron negociados por el personal técnico del CNE y los representantes de los partidos durante las auditorías, al margen de los acuerdos concretados en forma previa. A partir de conversaciones con representantes de los partidos políticos, y de la comparación de las actas oficiales con los informes de observación de fuentes ajenas al CNE, la Misión del Centro Carter puede inferir que durante esas auditorías se plantearon una serie de cuestiones sobre los procesos observados, lo que por lo general llevó a una serie de negociaciones y acuerdos. Los procesos de auditoría, por lo tanto, se fueron adaptando sobre la marcha, conforme a esos acuerdos verbales.

Si bien esta característica puede ser considerada un indicio de la buena voluntad del CNE para responder a las peticiones e inquietudes de los partidos políticos, la misma complicó el proceso de auditoría ya que los auditores y los observadores, locales e internacionales, no pudieron prepararse adecuadamente con antelación para dichas sesiones.

Una queja frecuente de los representantes de la oposición fue que el CNE no dio respuesta a las preguntas elevadas por ese sector, como así tampoco a las solicitudes de explicación de los procedimientos y procesos implementados para las elecciones del 3 de diciembre. El CNE, por ejemplo, no participó en un foro de Internet (una herramienta fundamental para las preguntas y dudas más frecuentes previas a las auditorías), y las preguntas allí planteadas — más de 100– quedaron sin respuesta. Los representantes de los partidos políticos reconocieron sin embargo sin reparos que, una vez iniciadas las auditorías, el CNE cumplió con su solicitud de efectuar modificaciones, concertando incluso sesiones de auditoría adicionales, que originalmente no estaban previstas.

Auditorias pre-electorales

Las auditorías llevadas a cabo en el período previo al día de los comicios fueron las siguientes: auditoria del hardware; auditoria del código fuente; auditoría de infraestructura de transmisión, auditoría de producción de las máquinas y auditoria de pre-despacho. La Misión del Centro Carter observó sólo la auditoría de pre-despacho y el último día de la auditoría de producción de máquinas.

Auditorías del hardware (máquinas de votación)

Las auditorías del hardware tuvieron lugar el 11 y el 13 de octubre. Conforme a las actas oficiales, el 11 de octubre, personal técnico de los partidos políticos desmontó y revisó los componentes físicos del modelo 3000 de las máquinas de votación y "revisó el sistema operativo". El 13 de octubre se hizo la inspección del modelo 3300. De acuerdo a las mencionadas actas, en esta sesión se formateó uno de estos modelos y se realizó una instalación virgen del sistema operativo (Windows XP Embedded). Luego se creó una imagen de esa instalación (utilizando Norton Ghost) y se generaron tres *hashes* de esa imagen (MD-5, SHA-I, SHA-256).[63] Los valores *hash* se hicieron constar en las actas. De acuerdo con el CNE, tanto la máquina del modelo 3000 como la del modelo 3300 operan exactamente con el mismo software, de modo que la serie de valores *hash* debía servir para ambos tipos de máquina. Esos valores se utilizarían posteriormente para verificar que se instalara la misma imagen, sin modificaciones, en la totalidad de las máquinas de votación.

Auditorías de código fuente (software de las máquinas y del centro de totalización)

Según las actas oficiales, las auditorías del código fuente tuvieron lugar el 16 de octubre y el 30 de noviembre. Las auditorías del software de las máquinas de votación, por su parte, finalizaron el 31 de octubre. La mayoría de las auditorías del software

63 Esto constituye un ejemplo de los cambios ad hoc en el proceso mencionados anteriormente. Inicialmente, solo estaba previsto incluir el algoritmo MD5. Los algoritmos SHA-I y 256 se incluyeron a pedido de los partidos políticos.

del centro de totalización finalizaron a mediados de noviembre, a excepción de dos auditorías adicionales practicadas el 21 de noviembre y el 30 de noviembre, a sólo cuatro días de las elecciones. Los observadores de la Misión del Centro Carter no estuvieron presentes en ninguna de esas auditorías ya que, a excepción de la última, tuvieron lugar antes de que éstos llegaran a Caracas. Los observadores del Centro Carter no fueron invitados a la última sesión de auditoría del código fuente.

Si bien las revisiones controladas del código fuente ofrecieron a los auditores de los partidos políticos cierto acceso al código fuente, éstos no pudieron aplicar sus propias herramientas de diagnóstico.[64] Conforme a una entrevista informal con miembros del personal del CNE, los auditores de la oposición habían insistido inicialmente en el uso de sus propias herramientas, pero dado que éstas no pudieron verificar los valores *hash* por tandas, los auditores finalmente accedieron a utilizar la herramienta provista por el CNE. Al margen de esta circunstancia particular, la Misión del Centro Carter considera que la transparencia y la confianza de la ciudadanía en el proceso de auditorías podría mejorarse si se permite a los partidos políticos, y las organizaciones internacionales y locales de observación acreditadas, un acceso mayor y más exhaustivo al código fuente.[65]

Si bien las revisiones controladas del código fuente ofrecieron a los auditores de los partidos políticos cierto acceso al código fuente, éstos no pudieron aplicar sus propias herramientas de diagnóstico.

Auditoría de la infraestructura de transmisión

El 20 y el 24 de octubre, se llevó a cabo la auditoría de la infraestructura de transmisión en la oficina central del CNE. De acuerdo con las actas oficiales, la misma consistió en una presentación de los diferentes módulos de la infraestructura. De acuerdo a lo señalado en tales actas, puede inferirse que esa presentación fue de índole informativa, ya que probablemente se utilizó una de las presentaciones de PowerPoint que se usó durante una sesión informativa similar concertada para los observadores internacionales de la OEA, la UE y el Centro Carter.

Funcionarios electorales señalaron al equipo del Centro Carter, en forma verbal, que en este período se efectuó también una auditoria de la plataforma de telecomunicaciones, que incluyó la revisión de elementos tales como la "lista blanca", los archivos de configuración, los routers, los servidores RAS utilizados en el CNT1 y CNT2 y las rutas de las redes de CANTV, Movilnet y redescom.

Auditoría de "producción de las máquinas"

De acuerdo con las actas oficiales, la auditoría de "producción de las máquinas" tuvo lugar entre el 1 y el 23 de noviembre. Los observadores del Centro Carter sólo observaron los procedimientos llevados a cabo en la sesión correspondiente al último día.

El objetivo de esta auditoría fue seleccionar una muestra aleatoria del 0,5 por ciento de las máquinas de votación preparadas en el lugar de armado de las mismas (lo que corresponde a 164 máquinas de un total de 32.331), para su posterior uso en la auditoría de "pre-despacho", la que se llevó a cabo el domingo 27 de noviembre.

Durante la observación del último día de esta auditoría, los miembros del equipo del Centro Carter pudieron observar lo siguiente:

- Los auditores seleccionaron una muestra aleatoria de las máquinas mediante el método de "sacar papelitos." Si bien la utilización de este procedimiento muestral contribuyó en su momento a asegurar la transparencia del proceso, la Misión del Centro Carter recomienda al CNE considerar en el futuro la adopción de técnicas de muestreo más rigurosas;

64 A excepción de la herramienta para generar y verificar *hashes* MD5

65 Véase Rezende (2004) para un comentario sobre un proceso similar en Brasil.

- El tamaño de la muestra seleccionada a partir del universo total de máquinas (0,5 por ciento) parece arbitrario dado que no se estableció previamente con claridad el margen de error ni el nivel de confianza. Si bien el procedimiento relativo a la selección de las máquinas contó con el visto bueno de los representantes de los partidos políticos, la Misión del Centro Carter considera que el proceso de muestreo hubiera tenido más sentido si el margen de error y los niveles de confianza se hubieran establecido con anterioridad al proceso de auditoría;
- Los auditores no fueron testigos presenciales de la selección de las máquinas elegidas de la línea de producción ya que sólo se limitaron a recibirlas en la sala preparada a tal efecto. De acuerdo a las explicaciones provistas por funcionarios del CNE, las restricciones de acceso a las áreas donde se encontraban las líneas de montaje de las máquinas se debieron a razones de "seguridad industrial". Si bien tales razones son atendibles, la Misión del Centro Carter considera que el organismo electoral podría considerar en el futuro la adopción de procedimientos que, teniendo en cuenta la seguridad e integridad física de los auditores, permitan la participación activa de estos últimos en el proceso de identificación de las máquinas en las áreas de almacenamiento o montaje.

Auditoria de producción del tablero

Como parte de la auditoria de producción de máquinas, el día 3 de noviembre se llevó a cabo una auditoría de la producción del tablero sensible al tacto. De acuerdo con las actas oficiales, durante esta sesión se llevaron a cabo los siguientes procedimientos:

- Los auditores realizaron una selección aleatoria de tableros electorales sensibles al tacto de la línea de producción;
- Los auditores verificaron que la selección realizada presionando los botones del tablero sensible al tacto coincidiera exactamente con la imagen del candidato y del partido superpuesta sobre dicho tablero.

Auditoría "pre-despacho"

La auditoría pre-despacho, que tuvo lugar el 26 de noviembre, fue la auditoría más pública de la serie. La misma fue diseñada y organizada por la Universidad Central de Venezuela (UCV), con la que el CNE celebró un contrato para tales fines. Los observadores del Centro Carter estuvieron presentes en esta auditoría.

Durante el transcurso de este ejercicio, se probaron las 164 máquinas de votación que habían sido seleccionadas previamente durante la auditoría "de producción" mediante la muestra aleatoria del 0,5 por ciento.

El objetivo principal de la auditoria "pre-despacho" fue simular el proceso de votación que tendría lugar el 3 de diciembre, a fin de constatar que las máquinas de votación funcionaran correctamente y que los resultados de la votación electrónica registrados en las máquinas, y en el sistema central de totalización, coincidieran con los registrados en el comprobante de votación impreso por las máquinas (que debía ser verificado visualmente por el elector antes de ser introducido en la urna). Otro de los objetivos de la auditoria fue constatar que la versión del software instalada en las máquinas de votación sea exactamente igual a la versión que había sido auditada y aprobada por los representantes de los partidos políticos durante la auditoría del código fuente.

Descripción del procedimiento y observaciones:

La auditoría pre-despacho se realizó en el lugar que previamente se había llevado a cabo la auditoria de producción de las máquinas.[66] En la misma participaron los operadores de las máquinas de votación, los técnicos de soporte del CNE, los representantes de los partidos políticos y los observadores.[67]

66 Las instalaciones de la empresa AEROCAV, en el área conocida como "Filas de Mariche".

67 Cabe acotar que debido a la gran cantidad de gente y máquinas de votación que había en la sala de auditoría, no fue posible observar todas y cada una de las partes de la misma. Las observaciones tuvieron por lo tanto el carácter de controles al azar: los observadores recorrían el local y realizaban observaciones y entrevistas a medida que los diferentes participantes podían atenderlos.

Las "paletas" donde se encontraban las máquinas de muestra que debían ser auditadas ya habían sido identificadas y separadas el día anterior para acelerar el proceso de desembalaje (proceso observado por la Misión del Centro Carter), por lo que, para dar inicio al ejercicio, el personal del CNE y los representantes de los partidos políticos procedieron a quitar los precintos de las paletas, abrir las cajas y colocar las máquinas de votación en una serie de mesas, donde los operadores debían ingresar los votos bajo la observación de los representantes de los partidos políticos.

Dado que para este ejercicio sólo se habían dispuesto 48 mesas (presumiblemente debido a limitaciones tanto de espacio físico como del número de operadores), no fue posible configurar las 164 máquinas al mismo tiempo, por lo que la simulación del proceso de votación debió realizarse por tandas. Los operadores debieron por lo tanto simular la votación y transmisión de los votos en un primer grupo de máquinas; retirar y almacenar nuevamente ese primer grupo, y proceder a efectuar el mismo procedimiento en un segundo grupo, y así sucesivamente, hasta que todas las máquinas fueran probadas.

En cada uno de los grupos, los técnicos de soporte procedieron a configurar y preparar las máquinas para el proceso de votación de acuerdo a los procedimientos previstos. Además de seguir los procedimientos estándar para esta fase (conectar la boleta electrónica, conectar el botón de desbloqueo, etc.), los técnicos conectaron un teclado externo a cada máquina, por medio del cual ingresaron al menú de configuración del BIOS, protegido por una contraseña, donde cambiaron la hora del sistema de las máquinas de votación, adelantando la hora real—aproximadamente las 10 de la mañana—a las 3 de la tarde. El motivo aducido por el personal técnico del CNE fue que las máquinas estaban programadas para evitar que el día de la votación se transmitieran los resultados antes de las 4 de la tarde. Debido a que esta auditoria requería que la transmisión se hiciera antes de esa hora (en parte para dejar lugar para la siguiente tanda de máquinas) era necesario cambiar la hora.

Durante el proceso de configuración de las máquinas, los observadores de la Misión del Centro Carter pudieron constatar que algunas máquinas presentaron problemas menores, los cuales fueron solucionados por los técnicos.[68] Asimismo, se observó que algunas de las máquinas fueron auditadas con la tapa posterior abierta, lo que hacía posible un fácil acceso a los puertos de entrada/salida (en algunos casos, las tapas posteriores no tenían precintos de seguridad). Durante la jornada, se informó que cinco de las 164 máquinas de votación seleccionadas no habían funcionado (lo que equivalía al 3 por ciento), por lo que debieron ser reemplazadas por máquinas de contingencia.

En un pequeño subgrupo de máquinas (seis de las 164, lo que equivalía al 3,6 por ciento) se llevó a cabo un proceso de verificación de valores *hash* a fin de comprobar que el software instalado coincidiera con la versión auditada, aprobada y firmada digitalmente por los representantes de los partidos. Para tal fin, se conectó un teclado externo a las máquinas seleccionadas y, desde una memoria extraíble especial, se inició un sistema operativo Linux, que incluía el software de verificación de *hashes* del CNE y un archivo con los *hashes* registrados durante las auditorías de código fuente. Los valores *hash* generados por la ejecución de este software (correspondientes a los archivos que incluían el software de votación instalado en la máquina) fueron comparados con los registrados durante las auditorías de código fuente, imprimiéndose los resultados mediante la impresora interna de la máquina (previa visualización de los mismos en la pantalla). Al encontrarse una coincidencia, se imprimía la palabra "OK" al lado de

68 Los observadores de la Misión del Centro Carter, por ejemplo, notaron que una máquina no reconoció su memoria extraíble, por lo que fue necesario abrirla, quitar dicha memoria, volver a insertarla, e iniciar de nuevo la máquina (hecho esto, la máquina reconoció la memoria y comenzó a funcionar correctamente).

69 El procedimiento de auditoria específica una verificación *hash* final para estas seis máquinas después de que la transmisión se haya llevado a cabo; presuntamente, para verificar que ningún código ha sido alterado durante la transmisión al servidor tally; así como una inspección a fondo del hardware de varias máquinas escogidas por los representantes de los partidos. Ninguna de estas medidas fue observada por la Misión del Centro Carter, por lo que no se puede confirmar si ocurrieron o no. Por otra parte, observadores de la Misión del Centro Carter notaron un caso en que parecía que existían errores en el programa *hash* de verificación. Un técnico corrigió los errores hasta que el programa corrió y éxitosamente produjo el *hash* que a su vez fue impreso y aceptado, como acertado, por los representantes de los partidos.

cada nombre de archivo. En general, este proceso se desarrolló sin mayores problemas.[69]

Una vez que las máquinas estuvieron en funcionamiento, los operadores iniciaron el proceso de votación (imprimiendo el reporte de diagnóstico y el acta de inicialización en cero) y los participantes comenzaron a ingresar votos al azar en las máquinas, verificando que su elección se plasmara correctamente en los comprobantes de papel impresos por las máquinas. Los comprobantes fueron guardados en sobres especiales y las observaciones se registraron en un formulario (conocido como "acta de auditoria pre-despacho; parte I: ingreso de votos"), que fue firmado por todos los observadores del proceso. Un total de 50 votos fueron ingresados por cada máquina de votación.[70]

Los operadores registraron luego los votos emitidos para cada candidato en un segundo formulario (conocido como "acta de auditoria pre-despacho; parte II: planilla de conteo"), que fue igualmente firmado por los observadores del proceso. Después de finalizada la votación, y si eran las cuatro de la tarde, o más tarde, los operadores iniciaban el procedimiento para finalizar la votación e imprimían el acta de escrutinio, que se colocaba luego en un sobre. Si todavía no eran las cuatro de la tarde, los operadores esperaban hasta esa hora para comenzar el procedimiento de cierre.

En las condiciones reales de votación, una vez impresa el acta de escrutinio, cada máquina debía conectarse directamente con su correspondiente medio de transmisión. De acuerdo a los procedimientos previstos para la jornada electoral del 3 de diciembre, la mayoría de las máquinas debía hacerlo a través de líneas telefónicas fijas (20.615 mesas); en algunos casos, esta operación debía hacerse mediante un teléfono celular para transmisión vía CDMA 1X (7.681 mesas); y en una reducida cantidad de casos (4.035 mesas), donde no había ninguna posibilidad de comunicación, en lugar de transmitir la información directamente, debía extraerse la memoria extraíble de la máquina conteniendo los votos y trasladarla físicamente al centro de transmisión más cercano para transmitir desde allí al centro de totalización.

Debido a las limitaciones físicas de la sala de auditoria (las mesas donde tenía lugar la votación no contaban con líneas telefónicas), los operadores procedieron a reproducir el caso de votación en lugares alejados sin conexión, quitando las memorias extraíbles de sus máquinas y trasladándolas al "centro de transmisión" de la sala, que consistía en una mesa con una pequeña cantidad de máquinas de votación especiales conectadas a una línea telefónica fija.[71] Estas máquinas operaban con un software especial, que sólo permitía la transmisión de los votos, no su emisión (el software fue teóricamente el mismo que se instaló en las máquinas de votación de los centros de transmisión de contingencia—CTC—el día de las elecciones).

El personal técnico que se hallaba en el "centro de transmisión" procedió entonces a transmitir los votos contenidos en la memoria extraíble al servidor de totalización. El informe de transmisión se incluyó en un sobre junto con las actas y documentos.[72]

Los sobres con las actas, así como las memorias extraíbles, se llevaron luego a la "mesa de coordinación", donde el personal del CNE, los auditores y los observadores compararon los votos registrados en el acta de escrutinio generada por la máquina con los resultados que constaban en los comprobantes de papel. Si no se encontraban discrepancias, se imprimía un resultado final de comparación que se guardaba junto con los sobres y las memorias extraíbles. En caso de hallarse discrepancias, se realizaban nuevos conteos para corregir posibles errores humanos. Si los errores persistían, debía

70 En una serie de máquinas, los votos ingresados no fueron aleatorios, sino que se ingresaron siguiendo una lista de votos predeterminada, que fue acordada de antemano con los representantes de los partidos. Estas listas predeterminadas podían contener una cantidad diferente de votos (en lugar de 50).

71 Otro método de conexión que se utilizó fue un teléfono celular conectado a través del puerto serial de una máquina de votación del "centro de transmisión".

72 En un caso observado, la máquina de votación conectada mostró correctamente que la memoria extraíble, una vez insertada, contenía votos de un proceso de votación cerrado, que todavía no había sido transmitido. Luego transmitió con éxito sus actas al centro de totalización. Utilizando una interfaz *Web* para mostrar resultados en tiempo real provenientes del centro de totalización (ubicado en la oficina central del CNE), se pudo verificar que el contenido de sus actas había sido transmitido correctamente. Al intentar transmitir las mismas actas una vez más, el centro de totalización aceptó la comunicación, pero señaló las actas como "ya recibidas."

consultarse a un supervisor para resolver la situación. De acuerdo a lo observado por la Misión del Centro Carter no parecía existir un proceso definido para solucionar errores generados por la máquina que no fuera el de "llamar al supervisor".

Por ultimo, una vez que los resultados se habían transmitido, y éstos habían llegado al servidor de totalización en el centro de conteo, los mismos fueron comparados con los resultados del conteo manual registrado en el informe de comparación a través de una interfaz *Web* segura (https), que consulta la base de datos del servidor de totalización.

Sumario de observaciones

Si bien, en general, durante la auditoría pre-despacho no se presentaron inconvenientes, los observadores de la Misión del Centro Carter pudieron notar los siguientes problemas:

- *Sólo se verificaron los hashes del software de una cantidad limitada de máquinas*. Durante el ejercicio de auditoría, sólo se verificaron los *hash*es del software de votación de seis de las 164 máquinas auditadas, lo que, en sentido estricto, indica que únicamente se pueden tener en cuenta esas seis máquinas para demostrar que el software inspeccionado, aprobado y firmado durante las auditorías de código fuente se instaló y funcionó correctamente.
- *La fecha del sistema no era la del día de la votación (se ajustó la hora, adelantándola hasta las tres de la tarde)*. Mientras que la hora de la máquina se adelantó hasta las 3:00 de la tarde, el calendario/reloj interno de la máquina no se ajustó para la fecha del día de las elecciones. Debido a que la eficacia de una prueba de esta índole depende de que se reproduzcan las condiciones de la jornada electoral, tanto la diferencia de fecha como el procedimiento de adelantar la hora constituyen fallas metodológicas importantes. Cualquier código maligno de gran complejidad (si el software del sistema tuviera alguno) utilizaría un mecanismo de activación específico para evitar activarse durante una situación de prueba (podría activarse, por ejemplo, mediante la fecha de la elección o el reloj interno de la máquina). Si tal código hubiera estado presente en las máquinas durante la prueba, el mismo podría haber sido programado para que se active poco después de la hora prevista para la apertura de los centros de votación (a las 9:00 de la mañana, por ejemplo,) y se desactive luego del mediodia (a las dos de la tarde, por ejemplo). Dado que las máquinas saltearon ese marco temporal, comenzando la prueba después de las 3:00 (además de operar el 26 de noviembre en lugar del tres de diciembre), ese código no se hubiera disparado durante la prueba, como lo hubiera hecho durante el día de las elecciones.
- *No se probaron todas las máquinas al mismo tiempo*. El hecho de que durante la prueba las máquinas de votación se retiraran y volvieran a almacenar por tandas, en lugar de configurarse todas a la vez, prolongó de manera innecesaria la duración de la auditoría y redujo la calidad del lugar en donde se realizó la prueba, generando un notorio y continuo movimiento de personal. Teniendo en cuenta la magnitud de la inversión que hizo el CNE para implementar su actual sistema automatizado de votación, sería tal vez recomendable disponer tanto de las facilidades físicas necesarias como de una cantidad suficiente de operadores, de modo que las máquinas seleccionadas puedan probarse todas al mismo tiempo.
- *Se estableció un límite de 50 votos*. Al igual que con el procedimiento de adelanto de la hora del sistema, el hecho de que la cantidad de votos ingresados tuviera un tope de 50 para la mayoría de las máquinas implica una diferencia significativa con las condiciones de la jornada electoral, durante la cual se pueden emitir hasta 600 votos. Un eventual código maligno podría activarse sólo después de haberse emitido una gran cantidad de votos, eludiendo así su detección durante la prueba. Los representantes de los partidos intentaron contrarrestar una posible amenaza de esta índole tratando de ingresar una gran cantidad de votos durante el período de votación de una hora.

- *Se contó sólo con una hora para el ingreso de los votos, lo que dio por resultado una alta velocidad de votación.* Un código maligno que se activara por la velocidad de votación tampoco podría haber sido detectado en esta prueba. El día de las elecciones, la votación se desarrollaría en forma mucho más lenta que la observada durante la prueba, y el código podría activarse solamente si la votación no excediera una cierta frecuencia, eludiendo así su detección en condiciones de prueba.

Debido a las deficiencias mencionadas, la auditoria "pre-despacho", aunque tal vez útil como una prueba más del sistema antes de las elecciones, y como un medio para generar confianza ciudadana, tuvo un valor limitado como instrumento para demostrar la integridad del sistema.[73]

Si bien en general no se presentaron mayores inconvenientes, los observadores del Centro Carter pudieron constatar la existencia de cierto nivel de confusión respecto de los procedimientos de la cadena de custodia.

Instalación de los centros de votación

El operativo de instalación de los centros de votación, que tuvo lugar el 1 de diciembre, no formó parte del plan de auditorías técnicas. El objetivo del mismo fue verificar el estado de las máquinas de votación y sus componentes (y reemplazar los componentes perdidos o dañados en caso que fuese necesario), a fin de evitar que se presentaran problemas el día de elecciones. Así, durante el transcurso de esta prueba se observó la entrega y recepción de las máquinas de votación en los lugares de votación, la configuración de prueba de las máquinas (para detectar errores y componentes faltantes) y la constitución de las mesas y autoridades electorales. La Misión del Centro Carter observó tanto un centro de votación seleccionado por el CNE,[74] como otros lugares de votación, seleccionados en forma aleatoria por el propio equipo de observadores de la Misión.

Si bien en general no se presentaron mayores inconvenientes, los observadores del Centro Carter pudieron constatar la existencia de cierto nivel de confusión respecto de los procedimientos de la cadena de custodia. Entre los participantes del ensayo se pudo observar asimismo mayor confianza en la pericia y autoridad de los operadores de las máquinas que en los propios funcionarios electorales. La Misión del Centro Carter pudo constatar además que el personal militar desempeñó un papel activo en el proceso de ensayo (lo que se notó particularmente en el lugar de votación seleccionado por el CNE).

En el centro seleccionado por el CNE, la totalidad de los precintos de seguridad de las cajas de las máquinas estaban rotos. Cuando se descubrió este hecho, los operadores de las máquinas adujeron que habían tenido que abrir las cajas el día anterior durante la entrega de las mismas, y que eso era parte del procedimiento. La Misión del Centro Carter constató no obstante que los procedimientos oficiales exigen que las cajas permanezcan cerradas y precintadas cuando se reciben (aunque esto se contradice con el manual del operador, que requiere un "inventario de todos los componentes de las máquinas," sin dejar en claro que ello deba hacerse en presencia de las autoridades de mesa y los testigos *durante* el operativo de instalación de lo centros y no antes).

En respuesta a la preocupación expresada por las autoridades de mesa, los operadores, adujeron que se había enviado una invitación para que dichas autoridades estuvieran presentes el día anterior en el momento en que se abrían las cajas y que ninguno de ellos había asistido pese a haber sido notificados. Los

73 Para una crítica similar de los procedimientos de "voto paralelo" en Brasil durante el día de las elecciones, véase Rezende (2004).

74 Colegio Nuestra Señora de la Consolación, en Caracas.

funcionarios electorales argumentaron que no recibieron tal invitación.

A fin de mitigar las preocupaciones, el oficial responsable del Plan República intervino afirmando que el día anterior "no había ocurrido ninguna irregularidad", que había "observado todo" y que podía "garantizar que el proceso había sido correcto." Dado que algunas autoridades de mesa seguían expresando dudas, señaló que, de cualquier modo, "el día de las elecciones las máquinas imprimirían un acta de inicialización en cero, que constituiría la prueba final de que no había habido ningún tipo de manipulación" porque de lo contrario ello "allí aparecería." Esta afirmación aparentemente tranquilizó a las autoridades de mesa, que no tomaron ninguna medida en presencia del equipo del Centro Carter. La confusión observada por la Misión del Centro Carter sugiere sin embargo que las autoridades de mesa, los operadores de las máquinas, los funcionarios electorales y los oficiales del Plan República se beneficiarían con una orientación más clara en lo que respecta a los roles y responsabilidades del personal electoral durante este operativo, así como también con procedimientos relativos a la cadena de custodia mejor definidos y uniformemente articulados.

Los miembros del equipo del Centro Carter concurrieron a otros lugares de votación sin anunciarse. En general, los observadores notaron que el ambiente era menos confuso que en el primer centro de votación. Si bien en varios casos se observaron irregularidades de menor importancia (tales como precintos rotos), las mismas no fueron lo suficientemente graves como para socavar la integridad del ejercicio.

Auditoria realizada durante el día de la elección

Luego del cierre de la votación y la transmisión de los resultados, en la totalidad de los centros de votación se llevó a cabo un sorteo, a fin de determinar las mesas que debían ser sometidas a la llamada auditoría "en caliente" o "de cierre". El sorteo se realizó en base a una tabla confeccionada por el CNE (ver Cuadro 2), utilizándose para ello el método de "sacar papelitos".

Número de máquinas en un centro de votación	Máquinas a ser auditadas
1 a 2	1
3 a 5	2
6 a 8	3
9 a 10	4
Más de 10	5

Cuadro 2. Tabla confeccionada por el CNE

Una vez realizado el sorteo, los miembros de mesa procedieron a contar en público los comprobantes de papel correspondientes a las máquinas seleccionadas, registrándose tanto el número total de comprobantes como los votos en cada uno de ellos. El resultado de ese proceso se volcó luego en el documento oficial de auditoría y se incluyó junto con los demás documentos oficiales para su posterior presentación al CNE.[75]

El procedimiento de auditoría "en caliente" no incluyó comparación alguna entre los resultados del recuento manual y el acta de escrutinio impresa por la máquina se votación, por lo que el procedimiento se limitó, en realidad, a una transcripción de los contenidos de los comprobantes en un documento oficial. A pesar de esta circunstancia, en la mayoría de los centros de votación observados por el equipo del Centro Carter, las autoridades de mesa y los testigos compararon por iniciativa propia, y en forma espontánea, los resultados del recuento manual con el acta de escrutinio impresa, llevando así a cabo lo que de hecho podría denominarse una auditoría parcial. No obstante ello, no existió un mecanismo formal para ese procedimiento, ni un documento que permitiera el registro de los resultados o describiera los procedimientos a seguir en caso de que se presentaran discrepancias entre los dos resultados.

La Misión del Centro Carter no tiene conocimiento de ningún caso en el que, durante este procedimiento, se hayan comparado los resultados locales (compro-

75 Este procedimiento, si bien no puede definirse exactamente como una "auditoria", el mismo forma parte del conjunto básico de contramedidas para evitar el fraude, definidas en Norden et al (2006) p.26

Observación del Centro de Totalización y el Centro de CANTV

Además de la observación de las auditorías pautada para el día de las elecciones, durante la jornada electoral los observadores de la Misión del Centro Carter observaron parcialmente los procedimientos efectuados en el Centro de Control de Redes de CANTV el día de la elección. Las actividades desarrolladas en el centro de totalización del CNE, sin embargo, no pudieron ser observadas debido a una decisión del organismo electoral relativa a "cupos" para la observación internacional.

Centro de Totalización

Dos observadores (uno de la Unión Europea y otro de la OEA) estuvieron presentes en el centro de totalización de la sede central del CNE durante varias horas el día de la votación observando el monitoreo del sistema, el ingreso de los datos de la votación, los IDS, etc. Dado que el CNE decidió permitir la presencia de solamente dos observadores internacionales en el centro de totalización, la Misión del Centro Carter no estuvo presente. Los observadores allí presentes compartieron sin embargo sus observaciones con el equipo del Centro Carter. Según su reporte, en dicho centro no se observó ninguna actividad irregular.

Centro de Control de Redes de CANTV

Un observador del Centro Carter tuvo oportunidad de estar presente en el Centro de Control de Redes de CANTV y observar durante varias horas el tráfico de red del sistema. La observación fue sin embargo interrumpida cuando las autoridades del CNE negaron el reingreso al observador después de que éste se hubiera tomado un descanso.

Los detalles de la observación hasta ese momento, incluidos los números concretos de tráfico observados como también los gráficos y esquemas, se muestran en el Anexo II. El siguiente es un resumen de los resultados:

- hasta aproximadamente las 18:00, no se observó ningún tráfico inesperado.
- poco antes de la interrupción de la observación, se advirtió una nivelación en el número de máquinas que transmitían los votos.

Este cambio repentino e inesperado en el tráfico de la red coincidió con informes de centros de votación de todo el país, según los cuales en muchos centros de votación el CNE o el Plan República pidieron a las autoridades de mesa que retrasaran el cierre de las mesas de votación (y por ende, la transmisión) a fin de permitir que votara un mayor número de electores.

bantes de papel o acta de escrutinio) con los resultados recibidos en el servidor central de totalización el día de la elección. Esta comparación se llevó a cabo al día siguiente, durante la auditoría post-electoral.

Auditoría Post-Electoral

Con el objeto de llevar a cabo la llamada auditoría post-electoral, al mediodía del día de las elecciones, con la presencia de representantes de partidos políticos y observadores, en la sede central del CNE se llevó a cabo la selección al azar de un uno por ciento de los centros de votación.[76] Dicha selección se realizó en forma similar a la realizada durante la auditoria de "producción de las máquinas", es decir, mediante el método de "sacar papelitos". Si bien este recurso muestral permitió la participación de los

76 Lo que equivalió a 106 centros (o alrededor del 0,5 por ciento del universo total de las máquinas de votación).

actores en el proceso de auditoría, resulta dudoso que, cuando se solicitó a los participantes que "verificaran" el procedimiento, éstos hubieran podido detectar números no secuenciales o números faltantes en un universo de más de 10.000 papelitos (uno por cada centro de votación).

La auditoria fue diseñada y organizada por la Universidad Central de Venezuela (UCV), con la cual el CNE había celebrado un contrato para ese propósito. La misma se llevó a cabo, en forma centralizada y bajo condiciones controladas, en las instalaciones de AEROCAV, ubicada en el área conocida como "Filas de Mariche". El proceso contó con la presencia de representantes de los partidos políticos, organismos nacionales e internacionales de observación y medios de comunicación.

De acuerdo al protocolo establecido para este ejercicio, del uno por ciento de los centros de votación seleccionados en la sede del CNE el día de las elecciones, sólo se tomaron en cuenta las máquinas que ya habían sido auditadas "en caliente" luego de la votación. Dado que faltaban 14 máquinas (que fueron reemplazadas por "máquinas de reserva"), en realidad sólo se auditaron 161 de las 175 máquinas seleccionadas. Otras cinco no pudieron ser auditadas debido a la falta de la documentación pertinente.

Durante esta auditoria, se contaron nuevamente los comprobantes de voto correspondientes a las máquinas auditadas. Los resultados de ese recuento se compararon con el registro de la auditoria "en caliente" generado por las autoridades de mesa el día de la elección, el acta de escrutinio que imprimieron las máquinas y los resultados recibidos en el sistema central de totalización. Por sus características, el procedimiento descrito se ajusta a la idea básica de una auditoría de rutina de los registros de los comprobantes verificados por el elector en el momento de la votación. Se trata de un tipo auditoría requerido cada vez más en el plano internacional. En algunos países, su realización constituye incluso un requisito legal.[77]

Los pasos seguidos durante esta auditoría fueron los siguientes:

- Los equipos de auditores recibieron los comprobantes de voto y las impresiones de las actas de escrutinio correspondientes;
- Los equipos contaron dichos comprobantes registrando los votos en actas confeccionadas para esta auditoría y las compararon luego con las actas de la "auditoria en caliente" completadas por las autoridades de mesa el día de la elección y con el acta de escrutinio impresa por la máquina;
- En caso de que los recuentos coincidieran, los documentos eran llevados a la "mesa de coordinación" para compararlos posteriormente con los resultados obtenidos en el centro de totalización. Si los recuentos no coincidían, se procedía a volver a contar. Si el recuento mostraba todavía discrepancias, se asumía que algunas de las boletas originales se habían perdido, por lo que los equipos de auditores usaban el "chorizo" (las copias de resguardo de los comprobantes de voto originales) para corregir los resultados de los comprobantes originales. Por lo general, el total de copias de resguardo no se contaba. Los equipos de auditoria buscaban los comprobantes de voto faltantes entre las copias de resguardo y cuando los hallaban utilizaban éstos en lugar del "original faltante". En caso de que persistieran las discrepancias después del conteo inicial, se ordenaban más recuentos. Los equipos volvían a contar hasta que los números coincidieran con las actas de escrutinio impresas (por lo general se alegaba que "era sumamente probable que existiera error humano"). Los procedimientos especificaban que, después de un número determinado de conteos infructuosos, la discrepancia debía hacerse constar en las actas de auditoría. No se

77 En los EEUU, 13 estados obligan a realizar algún tipo de auditoría de rutina de los registros de los comprobantes verificados por los electores, a fin de comprobar la precisión de las máquinas de votación. En esos estados, después de cada elección debe auditarse entre 1 y 10 por ciento de todas las máquinas de votación del distrito electoral. Véase www.verifiedvoting.org y (Norden et al, 2006, p16).

especificaban sin embargo los procedimientos para esos casos, ni consecuencias posteriores.

- Por último, los resultados del recuento de comprobantes se comparaban con los resultados registrados en la base de datos del centro de totalización. Para efectuar esa comparación se desarrolló una aplicación Microsoft Access, que había sido instalada en una serie de laptops en la sala de auditoría. Según el personal responsable de la UCV, el CNE había enviado ese día los resultados recogidos de la base de datos del centro de totalización por correo electrónico como un archivo de texto plano a uno de los miembros del personal de la UCV. El archivo adjunto descargado fue ingresado luego como referencia a la aplicación MS Access. Según las entrevistas realizadas en el lugar, ningún observador ni testigo de los partidos estuvo presente durante la recolección de datos. Tampoco se habían tomado medidas de seguridad para resguardar la integridad de los archivos.

Los observadores de la Misión del Centro Carter notaron varios casos de discrepancias menores, que fueron mayoritariamente consecuencia de comprobantes de votos en blanco que no habían sido depositados en la urna (véase la sección sobre usabilidad). Estas discrepancias se corrigieron utilizando las copias de resguardo de los comprobantes de voto del "chorizo". Durante la comparación con los resultados del centro de totalización se presentaron algunas discrepancias, que fueron debidamente registradas en las actas.

El grado de discrepancia no fue amplio: osciló entre el 0 por ciento (estado Amazonas) y un máximo de 1,62 por ciento (estado Trujillo). El promedio, por lo tanto, fue 0,19 por ciento (110 discrepancias sobre 57.505 votos contados).[78] Aparentemente, no se determinaron pautas respecto de los márgenes de error aceptables con anterioridad al ejercicio. En opinión de la Misión del Centro Carter, el establecimiento de tales pautas en futuras elecciones contribuiría a aumentar la transparencia general de las auditorías post-electorales.

Los observadores de la Misión pudieron observar que el propósito de la auditoría, como herramienta analítica crítica y relevante para fomentar la integridad del proceso electoral, no parecía estar claro para gran parte del personal de auditoría. La auditoria había comenzado tarde y los auditores parecían sufrir de "fatiga de auditoría".

El CNE informó a los miembros de la Misión del Centro Carter que en el informe final de auditoría de la UCV se incluirían los registros de auditorías no agregadas (por mesa de votación, con trascripción de comentarios del día de la elección registrados por las autoridades de mesa), por lo que esa información podría solicitarse una vez publicada.

Formateo de las memorias extraíbles y de las máquinas

El día después de la auditoría post-electoral, las memorias extraíbles y las memorias internas debían ser formateadas a fin de "impedir la manipulación de los datos." El proceso de formateo debía ser observado por testigos y auditores de los partidos.

Representantes de los partidos de la oposición manifestaron a los observadores del Centro Carter que el CNE había estado de acuerdo en permitir que ellos auditaran ciertas máquinas "problemáticas" antes de que se borrara la información, incluidas las máquinas con los precintos rotos (se informaron 169 casos) y aquellas que habían sido ubicadas en centros de votación donde testigos de la oposición habían informado acerca de irregularidades. Todas esas máquinas serían auditadas, independientemente de que el centro donde se encontraban hubiera sido seleccionado para una auditoría post-electoral, e independientemente de que la máquina hubiera sido seleccionada para una auditoría en caliente. Esta auditoría debía incluir la verificación de los *hashes* del software instalado para comprobar si había tenido lugar alguna modificación en el software. El equipo de observadores del Centro Carter abandonó Caracas antes de que esa revisión se llevara a cabo.

78 Datos obtenidos a partir de la observación de las pantallas de computadoras durante la auditoría.

Resumen de recomendaciones

- Negociar procedimientos completos de auditoría con los partidos políticos con anterioridad al proceso de auditoría. Esto permitiría a los auditores prepararse adecuadamente para las auditorías y fomentaría una mayor transparencia.
- Durante las auditorías del código fuente, los auditores de los grupos de observación y de los partidos políticos acreditados deberían tener acceso total e irrestricto al código fuente. Esto permitiría un proceso de auditoria más significativo que la revisión actual.
- Suministrar documentación detallada y completa del sistema a los auditores acreditados antes del plan de auditorías de modo que puedan prepararse de forma adecuada.
- El tamaño de la muestra para las auditorías predespacho y post-electoral debería determinarse conforme a principios estadísticos apropiados. Esto permitirá extrapolar los resultados para la totalidad de las máquinas de votación.
- Durante la "auditoria en caliente" del día de las elecciones, debería realizarse una comparación entre el conteo de comprobantes de papel con el acta de escrutinio impresa por las máquinas como parte obligatoria del procedimiento. Los resultados de los comprobantes de papel auditados también deberían analizarse mediante procedimientos estadísticos, y deberían implementarse procesos claros para los casos en que existan discrepancias entre las boletas de papel y los resultados electrónicos.
- Permitir que los resultados del recuento de boletas electorales constituyan la base de un cuestionamiento legal de los resultados electrónico.

Conclusiones y recomendaciones

Debido a su corta duración, y su reducido tamaño, la Misión de Observación Técnica del Centro Carter, no realizó una evaluación exhaustiva de la integridad del sistema de votación electrónica. Consecuentemente, en este informe sólo se ofrece un panorama general de los principales hallazgos de la misión en aquellos aspectos del sistema que los observadores pudieron analizar y observar. Sobre la base de esos hallazgos, y con la intención de cooperar con el Consejo Nacional Electoral, y el pueblo de Venezuela, el Centro Carter sugiere las siguientes recomendaciones, que espera puedan contribuir al desarrollo continuo de un proceso electoral sólido en Venezuela.

El diseño de las máquinas de votación

En los lugares de votación visitados por el equipo del Centro Carter se observó un razonable nivel de comprensión de la tecnología por parte del electorado, el cual, en general, pudo emitir su voto sin inconvenientes. Dada la introducción relativamente rápida, y a amplia escala, de las máquinas de votación electrónica, tal circunstancia es encomiable. La Misión del Centro Carter observó sin embargo cierta confusión entre los electores que afirmaban no haber podido emitir un voto en blanco o haber votado en blanco por accidente. El Centro Carter sugiere que el CNE considere eliminar el cambio de paradigma del proceso de interfaz de usuario para el voto en blanco. Cuando se emite un voto, la máquina determina que el tablero sensible al tacto es el lugar donde el elector realiza su elección y la pantalla táctil es el lugar donde se visualiza y se confirma esa elección. Para emitir intencionalmente un voto en blanco, el proceso debería ser el mismo. El tablero sensible al tacto debería contar con un botón separado para "voto en blanco", y esa opción debería visualizarse y confirmarse en la pantalla táctil, al igual que en el caso de los otros votos.

La impresión de un comprobante de voto, que el elector debe colocar en una urna luego de verificarlo, constituye un rasgo fundamental del sistema para el resguardo de la transparencia del acto eleccionario. La inclusión de este mecanismo en el diseño de las máquinas por parte del CNE es digno de elogio. Sin embargo, los observadores de la Misión del Centro Carter fueron testigos de algunos casos en que los electores se llevaron sin querer el comprobante de voto del lugar de votación. La falta de estos comprobantes de voto se observó luego en algunas de las auditorías post-electorales cuando se descubrieron discrepancias menores entre el conteo de los comprobantes de papel y los resultados electrónicos. La eficacia del comprobante de voto como herramienta que permita asegurar que las máquinas cuentan los votos del electorado con exactitud podría mejorar si se refuerza la capacitación de los miembros de mesa, a fin de minimizar el extravío de los comprobantes de votos. Las autoridades electorales podrían además considerar en el futuro la posibilidad de eliminar la manipulación de los comprobantes de voto mediante la adopción de tecnologías que sólo muestren el comprobante de papel al elector, sin permitirle tocarlo (detrás de un vidrio, por ejemplo).

El actual sistema no prevé procedimiento alguno para los casos en que el elector alega que el comprobante de voto no refleja el sentido de su voto. Dado que esta circunstancia atenta contra el sentido original de la verificación, el Centro Carter recomienda que el CNE considere modificar el sistema, de modo tal que el elector pueda cancelar o anular su voto en caso de que éste alegue que el comprobante impreso no refleja lo escogido en la pantalla. Mediante esos procedimientos, el voto electrónico podría ser borrado, y el comprobante invalidado, ya sea a través de su destrucción física o mediante la impresión de una nota de cancelación.

El diseño de la hoja de papel que está ubicada sobre el tablero electrónico sensible al tacto incluye fotografías de los candidatos, lo que, en el caso de los electores analfabetos, permite que éstos puedan emitir su voto sin recibir ayuda. Esta circunstancia constituye un instrumento importante para proteger el derecho humano universal al secreto de voto. El comprobante de voto, sin embargo, no incluye esas características. El CNE podría considerar tomar medidas para proteger aún más ese derecho incluyendo fotografías de los candidatos y símbolos de los partidos en el comprobante de voto. Esta medida permitiría que los electores analfabetos confirmen su propio comprobante de voto sin recibir ayuda. Las impresoras de los dos modelos de máquinas permiten una resolución de imagen de 200dpi como mínimo, lo que debería ser suficiente para obtener una imagen rudimentaria tanto del candidato como del símbolo.

De acuerdo a lo estipulado por el CNE, los electores cuentan con sólo dos períodos de tres minutos cada uno para emitir su voto. Esta circunstancia podría limitar la posibilidad de que un elector emita su voto, lo que, a su vez, podría afectar el ejercicio del derecho a elegir. Por consiguiente, las autoridades electorales deberían reconsiderar el criterio de "dos períodos de tres minutos para votar" que se aplica actualmente. Los electores no deberían perder el derecho al voto debido a dificultades para entender la tecnología empleada. El Centro Carter alienta por lo tanto al CNE a buscar un equilibrio entre la necesidad de implementar medidas que mejoren la velocidad y eficiencia del sistema de votación electrónico y la protección del derecho individual del ciudadano a elegir.

La seguridad del sistema

El Centro Carter se muestra complacido de que el CNE haya tomado una serie de medidas significativas para proteger el sistema de votación electrónica contra ataques externos, tales como la encriptación de datos mediante algoritmos estándar y la implementación de mecanismos sofisticados de randomización de datos. Igualmente elogiable ha sido la aplicación de medidas que tienen por objetivo evitar la manipulación indebida de las máquinas y el material electoral, tales como la inclusión de un número de serie alfanumérico de 32 dígitos en cada comprobante de voto impreso. Si bien esta última medida impide la falsificación de los comprobantes de voto, los números no pueden ser leídos en forma automática, lo que, en caso de ser necesario, dificultaría la verificación de la autenticidad de los comprobantes de voto a gran escala. El CNE debería por lo tanto considerar la posibilidad de que el número de serie del comprobante de voto pueda ser leído por un dispositivo especial en forma automática (mediante la inclusión de un código de barras, por ejemplo). De este modo, el número de serie podría convertirse en un mecanismo de seguridad funcional, lo que permitiría que la autenticidad de los comprobantes de papel pueda ser verificada en poco tiempo y sin demasiado esfuerzo.

Si bien el CNE ha hecho hincapié en las soluciones tecnológicas de seguridad, podría ser beneficioso que, en futuras elecciones, se tomen medidas adicionales de seguridad física para proteger las máquinas contra cualquier acceso no autorizado. Entre otras cosas, el Centro Carter estima que debería dificultarse aún más el acceso a la máquina propiamente dicha, en especial a sus puertos. En ese sentido, el Centro Carter sugiere se considere la posibilidad de deshabilitar físicamente los puertos que no son esenciales (como el puerto Ethernet, por ejemplo), en lugar de deshabilitarlos exclusivamente mediante el empleo de software. Los puertos esenciales, como los puertos USB (que conectan la máquina con la memoria extraíble), podrían protegerse contra posibles intentos de manipulación de un modo más eficaz mediante precintos de seguridad que sean controlados sistemáticamente, y cuya violación conduzca al reemplazo obligatorio de la máquina de votación afectada. Idealmente, debería considerarse deshabilitar por completo el acceso a las partes sensibles del sistema, tal como el menú de configuración del BIOS. Si esto no fuera factible, podría considerarse la implementación de una política de acceso al sistema mediante contraseñas, que sea clara y de amplia

divulgación, así como también un registro de acceso confiable, y el análisis obligatorio de dichos registros de acceso, con consecuencias preestablecidas para el acceso no autorizado.

Con respecto a la llamada cadena de custodia, los miembros de la Misión del Centro Carter fueron testigos de varios casos en que los procedimientos previstos para este importante aspecto del proceso electoral no se entendieron con claridad, o no se aplicaron rigurosamente. Por esta razón, el Centro Carter estima que el CNE podría considerar la posibilidad de tomar medidas adicionales para mejorar los procedimientos de la cadena de custodia durante el traslado y el almacenamiento de las máquinas de votación. Idealmente, podría considerarse la posibilidad de que el CNE compartiera con organizaciones de la sociedad civil la responsabilidad por la seguridad durante la instalación y el almacenamiento de las máquinas, en lugar de dejarla exclusivamente en manos del CNE y el Plan República. El traslado de las cajas con las máquinas de votación, por ejemplo, así como de los documentos y actas oficiales, podría realizarse conjuntamente con los representantes de los partidos políticos.[79] Los procedimientos de la cadena de custodia podrían además darse a conocer a todos los involucrados en el proceso electoral, como así también deberían hacerse públicas las listas del personal encargado de la cadena de custodia, de modo que cualquiera de los actores pueda identificar cualquier violación de los procedimientos, y llevar así a la práctica el principio "cuantos más ojos ven, mejor".

El Centro Carter considera que sería igualmente beneficioso que la cinta de seguridad fuera del mismo tipo en todo el sistema electoral. La cinta debería incluir características que impidan la falsificación, y que se den a conocer a todas las partes involucradas en el proceso, de modo que se reconozca fácilmente cualquier irregularidad. De esta forma se extendería la responsabilidad por la cadena de custodia, logrando de este modo una mayor transparencia del sistema, y una mayor confianza en el mismo.

La misión del Centro Carter pudo constatar que el CNE hizo todo lo posible para proteger el sistema de ataques electrónicos externos. El Centro Carter considera sin embargo que sería importante agregar niveles de seguridad adicionales para proteger el sistema central de totalización (y otros aspectos del proceso electoral) contra posibles manipulaciones internas malintencionadas. El Centro Carter sugiere por lo tanto que el CNE considere la posibilidad de recurrir a una Autoridad de Certificación externa e independiente para la emisión de certificaciones que protejan las comunicaciones entre las máquinas de votación y el centro de totalización, en lugar de utilizar para ello a la Autoridad de Certificación del CNE. Recurrir a una autoridad de certificación externa e independiente mejoraría la seguridad de la transmisión de datos, aumentando a la vez la confianza de las partes interesadas en el sistema electrónico y en el CNE.

El plan de auditorías

El plan de auditorías del sistema electrónico de votación venezolano incluye una amplia serie de pruebas de hardware y software, diseñadas para fomentar la integridad del proceso electoral. Dada su amplitud y exhaustividad, este plan puede constituir una importante herramienta para asegurar que las tecnologías de votación electrónica funcionen conforme a sus especificaciones y objetivos. Tal como se señaló en este informe, una característica importante del proceso de auditoría fue la receptividad y flexibilidad del CNE para enmendar dicho proceso a solicitud de las partes una vez que el mismo estaba en marcha. Si bien esto constituyó un medio importante para que los partidos políticos y las organizaciones no gubernamentales participaran activamente en la determinación del curso del plan de auditorías, el Centro Carter recomienda que el CNE negocie los procedimientos de auditoría con los partidos políticos y las asociaciones civiles con

79 Esto también es recomendado como una medida fundamental de seguridad por Norton et al (2006) p. 77

anterioridad a la realización de los mismos. De esa forma, los detalles de tales procedimientos podrían documentarse por escrito, con el acuerdo explícito de las partes involucradas, y darse a conocer públicamente sin modificaciones posteriores. Ello permitiría que los auditores se preparen adecuadamente sobre la base de la metodología establecida, lo que facilitaría la observación estructurada del proceso. Esta medida contribuiría además a aumentar el compromiso de los partidos políticos de la oposición ya que, de esa forma, los mismos estarían más estrechamente involucrados en el desarrollo de las auditorías.

El proceso de auditoría se vería además beneficiado por la participación de un equipo de auditoría bien informado. Para ello, el CNE debería considerar suministrar documentación completa y detallada sobre el sistema a auditarse a los representantes de los partidos políticos acreditados y las organizaciones de observación electoral con antelación al cumplimiento del cronograma de auditorías. Los auditores podrían de esa forma prepararse adecuadamente para esa tarea, analizar concienzudamente la arquitectura del sistema e identificar posibles riesgos para la seguridad.

El Centro Carter sugiere además que durante las auditorías del código fuente, los auditores de los partidos políticos acreditados puedan tener acceso completo e irrestricto al código fuente.[80] Los auditores deberían además poder aplicar herramientas de auditoría apropiadas durante un período adecuado antes de las elecciones. Tal circunstancia permitiría una auditoría más profunda que el actual proceso de revisión de código.

La utilización de técnicas de muestreo aleatorio durante los procesos de auditoría implementados por el CNE contribuyeron a aumentar la credibilidad de tales procesos. Estas, sin embargo, no se utilizaron uniformemente en la totalidad del proceso. En ese sentido, el Centro Carter desea sugerir que la muestra para las auditorias "pre-despacho" y post-electoral se mida y seleccione utilizando un marco estadístico apropiado. Esta medida contribuiría a asegurar que los resultados de la muestra puedan extrapolarse con confianza para el número total de máquinas de votación.

El CNE podría considerar además la posibilidad de determinar y dar a conocer públicamente el umbral de error aceptable para las auditorías antes de que éstas se inicien (siguiendo una metodología estadística estándar), en especial para las auditorías que comprueban la integridad tanto del sistema como de los datos. En el supuesto caso de que ese umbral de error se excediera, debería necesariamente concluirse que el sistema no funcionó correctamente, por lo que no podría verificarse la integridad del proceso. Para esos casos, el CNE debería determinar y divulgar, con anterioridad a las elecciones, las medidas a implementarse para solucionar este tipo de situaciones. Tales medidas podrían incluir un recuento de los comprobantes de voto, un proceso de auditoría a mayor escala, o incluso una repetición de las elecciones, según la magnitud del error cometido.

La implementación de una auditoría "en caliente" a gran escala el día de las elecciones por parte de las autoridades de la mesa electoral constituye una medida sumamente importante para asegurar la transparencia del sistema. La participación de la ciudadanía en ese proceso fomenta además la confianza en el proceso electoral. Por todo ello, el CNE merece un importante crédito. Las auditorías en caliente podrían sin embargo mejorarse en futuras elecciones si la comparación del resultado del recuento de los comprobantes de voto con el resultado del acta de escrutinio impresa por la máquina pasara a ser parte obligatoria del procedimiento. Los resultados podrían así regis-

80 Otro modelo consiste en utilizar un código fuente abierto. Los organizadores de la votación electrónica de 2001 del Territorio Capital de Australia adoptaron el modelo de código abierto y rechazaron las soluciones cerradas protegidas por copyright. El sistema eVACS fue desarrollado conjuntamente por una empresa privada y una universidad pública. Durante la programación, las versiones del software en constante evolución fueron subidas a Internet con regularidad, para que cualquier persona las bajara durante los seis meses del desarrollo del sistema. Cualquier persona podía tener acceso completo y gratuito a todo el código fuente, ejecutarlo, compilarlo, probarlo, aplicar herramientas especiales, etc. Los expertos en software y aficionados australianos que tenían interés ayudaron a evaluar el sistema e informaron sobre errores al equipo encargado del desarrollo. Varios errores se encontraron de esta manera, incluido un problema bastante serio, informado por un profesor de la Universidad Nacional de Australia. La versión final del software, que funciona bajo el sistema operativo de código abierto Linux, se publicó bajo la Licencia Pública General y desde entonces está a disposición del público (Zetter 2003, ACT 2001).

trarse en los documentos de auditoría oficiales.[81] Adicionalmente, los resultados de los comprobantes auditados podrían también analizarse para constatar si presentan anomalías estadísticas.[82]

El Centro Carter recomienda igualmente que el CNE introduzca medidas que apunten a solucionar eficazmente aquellos casos en que se presenten discrepancias evidentes entre los resultados del conteo de los comprobantes de voto y los resultados electrónicos.[83] Entre otras medidas se podría:[84]

- secuestrar y poner a resguardo las máquinas en que los resultados no coinciden;
- conducir una investigación pública de todas las máquinas que presenten discrepancias con el objetivo de identificar pruebas de posible manipulación;
- si se hallan pruebas de manipulación, ampliar la investigación e incluir *todas* las máquinas en que pudieran haber ocurrido problemas similares;
- identificar el número total de máquinas afectadas y analizar (sobre la base de mediciones estadísticas sólidas) si la cantidad de manipulaciones podría haber afectado el resultado de las elecciones;
- si la respuesta a la pregunta anterior es positiva, analizar la posibilidad de dictaminar una repetición de las elecciones.

El Centro Carter sugiere además el CNE considere la posibilidad de que los resultados del recuento de los comprobantes de voto realizado durante la auditoría "en caliente" puedan servir de base para un cuestionamiento legal de los resultados electrónicos de la elección cuando existan discrepancias importantes entre los resultados electorales manuales y los electrónicos. El CNE podría considerar además la posibilidad de adoptar un umbral estadísticamente significativo para tales las discrepancias. Las discrepancias que excedieran ese umbral podrían dar lugar a una investigación obligatoria a fin de identificar las causas de esa anomalía.

A fin de aumentar aún más la confianza de la ciudadanía en el proceso electoral, el Centro Carter sugiere además se considere la posibilidad de crear una organización de certificación autónoma con el objeto de certificar, de modo independiente, el sistema y la documentación del mismo y verificar así que el sistema cumple exactamente con las especificaciones publicadas por el CNE. Ese organismo de certificación podría además certificar la totalidad del sistema de voto electrónico respecto de su seguridad, y hacer recomendaciones para mejorarlo.[85]

81 En EEUU, por ejemplo, desde enero de 2007, trece estados exigen tanto los comprobantes verificados por los electores como la realización de auditorías manuales, o la extracción de una muestra aleatoria de máquinas que compare los resultados en papel con los electrónicos. Fuente: www.verifiedvoting.org.

82 Este análisis tendría el potencial de probar la existencia de manipulación. Véase Norden (2006) p. 76

83 Si una serie de registros simplemente invalida las demás, se estarían fomentando las manipulaciones de esa serie. Por ejemplo, si se privilegian los resultados electrónicos, un atacante podría concentrarse en cambiarlos y no necesitaría intentar también falsificar los registros de papel. Si los resultados en papel se privilegian, un potencial atacante tendría que concentrarse en manipular los resultados de los comprobantes de papel.

84 Véase Norden et al, (2006) pp. 74 -75; 90-92

85 En una entrevista, los auditores de la oposición afirmaron que se había propuesto la creación de un organismo independiente y multipartidario para desarrollar los planes de auditoría y certificar la tecnología, pero que, hasta el momento, dicha propuesta había sido rechazada por el CNE. Entre otros modelos se encuentra la Commission on Electronic Voting (Comisión de voto electrónico) de la República de Irlanda que tiene la obligación de proporcionar una evaluación independiente del funcionamiento del sistema de votación electrónico, particularmente respecto del secreto y la precisión de las tecnologías. Conformado por secretarios del condado, el presidente de la Science Foundation of Ireland y la Information Society Commission, este organismo no certifica la tecnología de votación electrónica propiamente dicha, sino que tiene la capacidad de revisar las pruebas de certificación que tuvieron lugar y de encargar nuevas pruebas (para mayor información, véase http://www.cev.ie/index.htm). El Center for Election Systems del estado de Georgia, EEUU, tiene su sede en una universidad. Conformado por académicos y profesionales técnicos, el centro realiza una prueba de validación independiente y capacita a personal de elecciones y operadores de máquinas (para mayor información, véase www.elections.kennesaw.edu). El Physikalisch Technische Bundesanstalt (PTB) de Alemania es un laboratorio independiente que funciona bajo el auspicio del Ministerio Federal de Economía y Tecnología. El PTB hace una verificación independiente de las soluciones de votación electrónica y de Internet y está elaborando guías para el desarrollo y prueba de sistemas de votación en línea (para mayor información véase http://www.ptb.de/index_en.html).

Una mayor participación de los partidos políticos en el proceso, en especial los de la oposición, podría aumentar la confianza de la ciudadanía en el CNE y en el sistema de votación electrónica. En este marco, se podrían añadir medidas de auditoría adicionales que, formando parte del marco regulatorio, la oposición podría ejecutar en forma independiente. Por ejemplo:

- a los auditores de la oposición se les podría brindar acceso a las máquinas de votación que ellos decidan durante las auditorías preelectorales, a fin de verificar los *hashes* del software que se ha instalado;
- si los testigos informaran de irregularidades graves en ciertos centros de votación, se podría garantizar a expertos de la oposición el derecho de inspeccionar las máquinas de esos centros;
- podría permitirse que los auditores de la oposición realicen una observación en el centro de totalización. Esto implicaría compartir el acceso a herramientas de monitoreo de resultados en tiempo real, así como a herramientas cruciales como el módulo PEM.

Lecciones para la observacion de elecciones electronicas

En la mayoría de los sistemas de votación electrónica, y especialmente en un sistema tan complejo y sumamente automatizado como el que se describe en este informe, la cantidad de aspectos que pueden observarse visualmente es limitada. A diferencia de las elecciones manuales tradicionales, un observador o un testigo de un partido puede estar de pié, al lado de una máquina de votación en uso, de una línea telefónica que está transmitiendo datos de la elección o de un servidor de totalización que está sumando y aun así no poder constatar si las computadoras están funcionando según las especificaciones establecidas y las expectativas del electorado. La observación de la interfaz de usuario en la máquina de votación (la observación de la pantalla para constatar que todo esté bien) no es en esencia capaz de detectar irregularidades ni fraude, dado que cualquier atacante trataría de ocultar sus acciones detrás de una cortina de humo de visualización de una interfaz de usuario del sistema aparentemente normal y correcta. El fraude electrónico, mientras se está llevando a cabo, es prácticamente invisible.

La observación de elecciones electrónicas por parte organizaciones internacionales debe por lo tanto poner énfasis en la observación de los procedimientos de auditoría, el diseño e implementación de los procedimientos relativos a la cadena de custodia y la comprensión de la arquitectura del sistema y el marco legal e institucional. La presencia de observadores el día de la elección, si bien sigue siendo importante, es insuficiente por sí sola. La observación de las auditorías, y el análisis subsiguiente de su calidad y amplitud, pueden arrojar resultados más significativos en cuanto al cumplimiento de las reglas durante las elecciones que las observaciones visuales tradicionales durante el día de la votación. Esto se vuelve especialmente cierto si la participación de la oposición y la sociedad civil en el diseño e implementación del sistema de votación electrónico es limitada, como sucede en Venezuela. En estos casos, las auditorías pasan a ser el medio principal para que sectores evalúen si el sistema electrónico de votación ha funcionado correctamente o si puede haber presentado irregularidades. En este escenario, la responsabilidad de brindar confianza sobre los resultados electorales recae casi por completo en el proceso de auditorías.

En cuanto a la metodología de observación para las elecciones electrónicas, queda mucho por hacer. La principal dificultad radica en la falta de coherencia que muestran las soluciones tecnológicas entre los distintos países y la complejidad de esos sistemas, si se los compara con los procesos de votación manual tradicionales. Los esquemas de auditoría también muestran gran variación. No resulta sencillo encontrar una metodología unificadora que sea aplicable a todos los sistemas y planes de auditoría y que sea suficientemente ágil para una utilización práctica durante una misión de observación.

No obstante, existen prácticas que se consideran las mejores y que un observador puede controlar. En auditorías de código fuente, por ejemplo, la mejor práctica es el acceso libre, completo y temprano a la totalidad del código fuente del sistema para los representantes de partidos políticos acreditados. En auditorías del tipo de comprobación paralela (caja negra/pruebas de datos), la mejor práctica consiste en aplicar métodos estadísticamente sólidos para determinar la dimensión de las muestras, verificar que la selección de esas máquinas de muestra haya sido realizada por el más puro azar y recrear condiciones de votación exactamente idénticas a las que se dan en los centros de votación el día de la elección. En las auditorías “en caliente” de los comprobantes de voto,

nuevamente se trata de conocer la dimensión de la muestra y contar con métodos confiables para compararla con los resultados electrónicos que se reciben en la central. Por ultimo, y aquí es aún muy relevante la observación en el día de la elección, una cadena efectiva de custodia—cuya responsabilidad compartan todos los involucrados y que debe estar celosamente protegida contra toda violación—constituye la médula de la seguridad electrónica. Para que la seguridad electrónica sea realmente significativa, también se requieren políticas de seguridad relacionadas con el acceso del personal y el conocimiento de contraseñas.

Más allá de ello, un importante indicador de la confiabilidad del sistema—independientemente de los detalles de la solución tecnológica que se aplique—es el grado general de centralización y unilateralidad existente en la toma de decisiones versus los enfoques participativos que involucren a todos los participantes. Los controles y equilibrios no dejan de ser relevantes por el hecho de que se haya ingresado a la era del voto computarizado.

El siguiente paso hacia una metodología de observación más uniforme de elecciones electrónicas es el desarrollo continuo de una lista de "preguntas a formular", muchas de las cuales no serán contestadas el mismo día de la elección sino con anterioridad a través del estudio de documentos y entrevistas.

Bibliografía

ACT (2001) The 2001 ACT Legislative Assembly Election Electronic Voting and Counting System Review, **Election Review Computer Voting**, http://www.elections.act.gov.au/adobe/.

Brunazo, A. (2004) **O Voto de Cabresto Póst Moderno**, http://www.votoseguro.org.

Caltech-MIT (2001). **Voting—What Is, What Could Be**, The CALTECH-MIT VOTING TECHNOLOGY PROJECT, http://vote.caltech.edu.

Calvo, E.: Escolar, M.; Pomares, J. (2007) "Split Ticket incentives under alternative e-voting advices: experimental evidence on information effects in multiparty elections," *American Journal of Political Science*, (de próxima aparición).

CNE (2006c) Manual Operativo para Miembros, Secretaria o Secretario de Mesa Electoral, Elección Presidencial 2006.pdf".

CNE (2006d) Instructivo dirigido a los Efectivos del Plan República, Elección Presidencial 2006, pdf.

CNE (2006a) Porqué su voto es secreto, Elección Presidencial 2006.pdf.

CNE (2006b) Manual del operador de máquina, Elección Presidencial 2006, pdf.

CNE (2006e) Tríptico OMV Elección V7, (13112006) Elección Presidencial 2006, pdf.

CNE (2006f) Official Minutes of the Audits of the Venezuela Presidential Elections, Presidential elections 2006. (juego de fotocopias).

Elklit, J. y Reynolds, A. (2002) "The impact of election administration on the legitimacy of emerging democracies: a new comparative politics research agenda," en: *Commonwealth and Comparative Politics*, Vol 40, Nº 2: 86-119.

Gobierno Ciudad Autónoma de Buenos Aires (2005) 2005. E-voting Pilot Project. First Evaluation Report. Executive Summary. Buenos Aires.

Hartlyn, J.; McCoy, J. (2006) "Observer paradoxes: How to Assess Electoral Manipulation," in: *The Dynamics of Electoral Authoritarianism*, (A. Schedler, ed.), Boulder (Co), Lynne Rienner, Pub.

Hartlyn, J; McCoy, J; Mustillo, Thomas (forthcoming 2008). "Explaining the Quality of Elections in Latin America." Comparative Political Studies.

Leohucq, F. (2003) "Electoral Fraud: Causes, Types and Consequences," *Annual Review of political science* 5: 233-256.

López Pintor, R. (2000) Electoral Management Bodies as Institutions of Governance, New York, United Nations Development Program.

Massicotte, L.; Blais, A.; Yoshinaka, A. (2006) *Establishing the Rules of the Game. Elections Laws in Democracies*, Toronto, University of Toronto Press.

Mercuri, R. (2002) "A Better Ballot Box? New electronic voting systems pose risks as well as solutions." *IEEE Spectrum Magazine* October 2002. Disponible en http://www.spectrum.ieee.org/WEBONLY/publicfeature/oct02/evot.html.

Neumann, P. (1993) *Security Criteria for Electronic Voting*, Proceedings of the 16th National Computer Security Conference Baltimore, Maryland, September 20-23, http://www.csl.sri.com/users/neumann/ncs93.html.

Neumann, P. (1995) *Computer Related Risks*, Addison-Wesley, http://www.csl.sri.com/neumann.

Norden et al. (2006). The Machinery of Democracy: Protecting Elections in an Electronic World, Voting Rights & Elections Series, Brennan Center for Justice at NYU School of Law, 2006.

RABA (2004) Trusted Agent Report - Diebold AccuVote-TS Voting System, http://www.raba.com/press/TA_Report_AccuVote.pdf.

Rezende, P. (2004) "Electronic Voting Systems: Is Brazil ahead of its time?" *CryptoBytes* (RSA Laboratories), Volume 7, No. 2, Fall 2004.

Schedler, A. (1998) "Delegation without discretion. The Bureaucratization of Electoral Administration in Mexico," Artículo presentado en el XXI Congreso Internacional de Latin American Studies Association (LASA), Chicago, 24-26 Septiembre.

Smartmatic S.A. (2006) Smartmatic Automated Election Systems—SAES_v3.2 101006.pdf.

Smartmatic, S.A. (2006a) SAES, Carter Centre.pdf".

Tadayoshi, Stubblefield, Rubin, Wallach (2003) Analysis of an Electronic Voting System, Johns Hopkins University Information Security Institute, Technical Report TR-2003-19, http://avirubin.com/vote.pdf.

Thompson, K. (1984) "Reflections on Trusting Trust." *Communication of the ACM*, Vol. 27, No. 8, August 1984, pp. 761-763, http://http://www.acm.org/classics/sep95/.

Zetter, K. (2003) "Aussies Do It Right: E-Voting." Wired Online News November 2003, http://www.wired.com/news/ebiz/0,1272,61045,00.html?tw=wn_story_page_prev2.

Anexo I
Metodología de observacion del Centro Carter

Debido su corta duración, y su reducido tamaño, la misión de observación técnica del Centro Carter no se propuso obtener resultados estadísticamente relevantes. En lugar de ello, intentó recolectar ejemplos y anécdotas a partir de las cuales poder extraer conclusiones aproximadas respecto de la influencia que los factores seleccionados por el equipo del Centro Carter tuvieron en el proceso electoral. Por la misma razón, los equipos de observadores del Centro Carter fueron alentados a observar el proceso electoral en su totalidad, centrándose en un grupo de uno a tres centros de votación durante el día y captando el proceso completo en uno de ellos. En lugar de hacer hincapié en la amplitud de la observación, se apuntó a la profundidad.

Los equipos de observadores del Centro Carter fueron enviados a los centros de votación sobre la base de tres variables: grado de participación esperado; grado de polarización esperado; y método de transmisión utilizado.

Variable 1: Grado de participación esperado

El objetivo de observar este factor fue evaluar el funcionamiento del sistema de votación en tres escenarios:

- Situación de alto uso (alta participación, muchos electores en rápida secuencia)
- Situación de bajo uso (baja participación, pocos electores)
- Uso normal (participación media)

Esta variable tuvo potencial impacto en el proceso de votación durante toda la jornada electoral.

Variable 2: Grado de polarización esperado

Esta variable está relacionada al porcentaje de los electores del partido oficialista versus los partidarios de la oposición (base de datos del referéndum de 2004). Este factor podía traducirse en los siguientes escenarios:

- Bajo grado de vigilancia en lo que respecta al uso de la tecnología (con gran mayoría del partido oficialista)
- Alto grado de vigilancia en lo que respecta al uso de la tecnología (con gran mayoría de la oposición)
- Control y vigilancia recíprocos (con fuerte competencia entre oficialismo y oposición)

Esta variable tuvo potencial impacto en los procedimientos de apertura y cierre, así como también en el proceso general de votación durante el día.

Variable 3: Método de transmisión utilizado

Para esta variable se tuvieron en cuenta las formas de transmisión utilizadas el día de la elección:

- Transmisión por línea telefónica fija
- Transmisión por teléfono celular
- Transmisión desde los Centros de Transmisión de Contingencia después del traslado manual

Esta variable tuvo potencial impacto en el cierre del proceso.

Dado que la ubicación geográfica tiene poca influencia sobre los factores seleccionados, se eligieron centros de votación cercanos (zona metropolitana de Caracas y el estado de Miranda). A fin de ampliar el alcance de la evidencia empírica recolectada, se seleccionó una serie de centros de votación de apoyo, cercanos a los principales. Durante los momentos de poca actividad en los centros principales, los equipos de observadores podían recorrer los secundarios. Los observadores debían estar presentes en el centro principal durante la apertura y cierre de la rotacion. De este modo, se esperaba maximizar la observación de la interacción de los electores con la interfaz de usuario de la máquina de votación a fin de evaluar la usabilidad de las máquinas en general.

Los resultados empíricos de la observación se utilizaron posteriormente para ilustrar diferentes aspectos del sistema de votación. En general, los observadores del Centro Carter notaron una mayor tensión en los centros en los que había paridad política, tal como era de esperarse. Los centros de votación del partido oficialista mostraron un bajo nivel de vigilancia y mayor cantidad de dudas técnicas, siendo más frecuentes los problemas con la interfaz de usuario. Los bastiones de la oposición por lo general presentaron operaciones poco conflictivas y un alto nivel de comprensión técnica con menos problemas respecto de la interfaz de usuario.

Anexo II
Detalle de las Auditorias

Auditorías del código fuente de las máquinas de votación

Según las actas oficiales, las auditorías del código fuente tuvieron lugar entre el 16 y el 31 de octubre de 2006. Los observadores del Centro Carter no estuvieron presentes en ninguna de ellas.

16 de octubre.

El Centro Carter no recibió las actas oficiales de los procedimientos del 16 de octubre. Según un breve informe de auditoría del GST, ese día se generaron *hashes* de los archivos del código fuente que serían auditados en las siguientes sesiones de auditoría. También se acordó un cronograma para esas sesiones.

17 de octubre.

Según las actas oficiales, sucedió lo siguiente:

- Se creó un "espacio de operación controlado" mediante la instalación de una imagen de Windows XP Embedded verificada por *hashes*, que había sido creada en una PC durante las auditorías previas;
- Se copió el código fuente de las "aplicaciones para las Elecciones Presidenciales 2006" en esa PC87;
- Se crearon *hashes* de esos archivos de código fuente y se compararon con los creados el 16 de octubre, a fin de asegurar que se auditaría el mismo código fuente;
- Se compilaron las siguientes aplicaciones: Election; InstallSAES; CTS; CFEncryptor; BallotProduction; SAESDataUtil;
- Las aplicaciones se protegieron utilizando una contraseña de múltiples partes (las que eran conocidas sólo por los respectivos participantes: una por los partidos políticos, otra por el CNE y otra por el proveedor, Smartmatic). Esto se realizó utilizando la aplicación "GenKeyAndProtect," la que se compiló en presencia de las partes;
- Se creó una serie de valores *hash* (Md5, SHA-I, SHA-256), tanto de las aplicaciones compiladas y protegidas como de los archivos del código fuente. Todos estos valores *hash* fueron almacenados en un archivo de texto denominado "Plantilla_Hashes_Binarios_y_Fuentes.txt", del cual nuevamente se generaron tres valores *hash* (Md5, SHA-I, SHA-256); esos valores se registraron en las actas;
- Se realizó una revisión visual de las partes del código fuente que incluían el esquema de encriptación utilizado en la máquina de votación, incluido el manejo de las contraseñas de contingencia.

Notas y observaciones:

No resulta claro si el software compilado en esa sesión incluye el del centro de totalización. A partir de la lista de aplicaciones compilada, no pareciera que fuera así. Al parecer, la revisión de código fue realizada "mostrando el código fuente" a los auditores en pantalla, y revisando las líneas del código fuente una por una. El código fuente no pudo ser llevado por los representantes de los partidos políticos y/o analizado mediante la utilización de sus herramientas.

18 de octubre.

Según consta en las acta oficiales, sucedió lo siguiente: después de verificar los valores *hash* respectivos, se encontró que la imagen del sistema operativo instalada en el ordenador utilizado para la auditoria "no tenía controladores de tarjetas de red"; se instalaron esos controladores; se creó una nueva imagen del sistema operativo (incluidos los controladores), y se generaron y registraron nuevos valores *hash* para esa imagen.

Notas y observaciones:

No queda claro por qué fue necesario agregar controladores de tarjetas de red. Según las especificaciones,

la máquina de votación no usa su tarjeta de red Ethernet incorporada para comunicarse durante el día de elecciones. Conforme a los procedimientos de seguridad, la tarjeta debería haberse deshabilitado en el registro de sistema porque la máquina no la necesita, y su presencia representa un riesgo innecesario para la seguridad. En consecuencia, lo lógico hubiera sido que la imagen del sistema operativo cuyo objetivo era la posterior instalación en las máquinas de votación no contuviera esos controladores.

19 de octubre.

Según consta en las actas oficiales, sucedió lo siguiente:

- "Revisión del proceso de votación";
- "Revisión del proceso de transmisión de votos"

Notas y observaciones:

No se incluyó más información en las actas oficiales.

20 de octubre.

Según consta en las actas oficiales, sucedió lo siguiente:

- "Revisión del proceso de votación";
- "Revisión del proceso de transmisión del acta de escrutinio";
- "Escrutinio";
- "Evaluación de las herramientas de prueba"

Notas y observaciones:

No se incluyó más información en las actas oficiales.

23 de octubre.

Según consta en las actas oficiales, sucedió lo siguiente:

- "Revisión del manipulador de entorno de las máquinas de votación";
- "Revisión del mecanismo que evita la reconstrucción de la secuencia de voto (utilizando NTFS explorer)";
- "Instalación de prueba de una máquina del modelo 3300";
- "Votación de prueba, generación del acta de escrutinio y comparación con los votos emitidos"

Notas y observaciones:

No se incluyó más información en las actas oficiales.

24 de octubre.

Según consta en las actas oficiales, sucedió lo siguiente:

- "Revisión del mecanismo de reemplazo de la memoria extraíble";
- "Revisión del mecanismo de reemplazo de la máquina de votación"

Notas y observaciones:

No se incluyó más información en las actas oficiales.

26 de octubre.

Según consta en las actas oficiales, se practicaron dos nuevos procedimientos de auditoría que habían sido solicitados específicamente por los representantes de los partidos. A solicitud de ellos, estos procedimientos fueron incluidos en el proceso de auditoría:[86]

- Tanto una máquina del modelo 3000 como una del modelo 3300 fueron iniciadas desde una memoria extraíble Linux y se ejecutó un script llamado "revisar-hardware.sh" que detecta todos los componentes físicos de la máquina de votación;
- Mediante una herramienta (Process Explorer), se identificó qué fueron usados por la aplicación Election. De los 89 dlls encontrados, 20 fueron dlls seleccionados como importantes y se generaron valores *hash* de todos ellos. Los valores *hash* fueron almacenados.

31 de octubre.

Tuvo lugar la última auditoria de software de las máquinas de votación. Según consta en las actas oficiales, sucedió lo siguiente:

86 Este es un ejemplo de los cambios al proceso ad hoc anteriormente mencionados.

- Se tomó una muestra del 1% de los archivos de configuración de las máquinas de votación (en texto claro);[87]
- Se encriptaron los archivos de la muestra mediante la aplicación CFEncrypter;[88]
- Se generaron valores *hash* de los archivos encriptados de las muestras, y se compararon esos valores *hash* con sus valores *hash* correspondientes a partir de una lista de todos los valores *hash* de todos los archivos de configuración encriptados, que fue previamente provista por el CNE;
- Se extrajo una lista de información no confidencial, solamente electoral, de los archivos de la muestra no encriptados, y se entregó esa lista a los representantes de los partidos;
- La mencionada lista de todos los valores *hash* de todos los archivos de configuración encriptados "se verificó en todas las 'burn stations'."[89]

Auditorías del código fuente del sistema central de totalización

Según consta en las actas oficiales, las auditorías del código fuente del Sistema Central de Totalización tuvieron lugar entre el 25 de octubre y el 30 de noviembre. Los observadores del Centro Carter no estuvieron presentes en ninguna de estas auditorías. Si bien la mayoría de las auditorías se llevaron a cabo antes de la llegada de los observadores del Centro Carter, dos de ellas se realizaron luego de la llegada del Centro Carter. Dado que no se informó que esas auditorías se estaban realizando, no fue posible acceder a ellas.

25 de octubre.

Según consta en las actas oficiales, tuvo lugar una sesión informativa inicial, en la que se presentaron los módulos funcionales del sistema de totalización central. Se acordó un cronograma inicial para las siguientes sesiones de auditoría del código fuente.

26 de octubre.

Según consta en las actas oficiales, sucedió lo siguiente:

- Revisión del módulo Receptor de actas;
- Inspección inicial del código fuente del módulo de recepción;
- Inspección de las tablas de la base de datos usadas por el módulo de recepción ;
- Se generó un valor *hash* del código fuente de "toda la aplicación";
- Se fijó un cronograma de inspección detallada para los módulos

27 de octubre.

Según consta en las actas oficiales, sucedió lo siguiente:

- Verificación del valor *hash* generado al finalizar la auditoria del 26 de octubre, para verificar que no se hubiera modificado ningún código;
- Revisión constante del módulo Receptor de actas;
- Revisión del flujo funcional que tiene lugar una vez que se recibe una transmisión desde una máquina de votación;
- Revisión del proceso de almacenamiento de la información electoral en la base de datos central, verificando los mecanismos de validación.

87 Se supone que estos archivos de configuración son los que estaban almacenados en la memoria extraíble que, una vez insertada en una máquina de votación "en blanco", copia los archivos de configuración en esa máquina y la configura de modo permanente para ese centro de votación y esa mesa específicos.

88 Esta es la misma aplicación que usa la máquina de votación para manejar sus archivos de configuración encriptados. Su autenticidad se verificó mediante valores *hash*.

89 Se supone que se trata de centros de copiado de memorias extraíbles.

30 de octubre.

Según consta en las actas oficiales,[90] se llevó a cabo una revisión detallada de la lógica de negocio del receptor de actas, que originó una tabla de casos de recepción, y su consiguiente manejo por parte del receptor de actas más los códigos de "estado" fueron guardados en la base de datos.[91]

31 de octubre.

Según consta en las actas oficiales, sucedió lo siguiente:

- Revisión del esquema de la base de datos;
- Otra revisión del módulo Consulta de resultados (basado en la *web*);
- Se llevaron a cabo pruebas de transmisión;
- Se ingresaron al sistema registros a partir de votos manuales, simulando aquella parte del proceso aplicable a las pocas mesas no automatizadas que se usarían.

3 de noviembre.

Según consta en las actas oficiales, sucedió lo siguiente:

- Se revisaron actualizaciones de diferentes versiones de software (módulo procesador de la base de datos y módulo "acta de escrutinio transmitida");[92]
- Una nueva revisión del modulo de informe de las actas por boletín;
- Revisión del modulo EMS que genera las Certificaciones de las máquinas de votación el día de las elecciones.

Notas y observaciones:

Las actualizaciones de las versiones no se especifican con más detalle, como tampoco se especifican las posibles consecuencias de esas actualizaciones en el proceso de auditoría. En la primera página de esas actas hay una observación, en la que se indica que las tres páginas que contienen preguntas aún sin responder habían sido presentadas por un representante de la oposición como parte de las actas. Ese anexo no se adjuntó a la copia que el CNE entregó al Centro Carter. Uno de los auditores de la oposición,[93] señaló al Centro Carter que durante algunas de las sesiones de auditoria del código fuente, los "apéndices" habían sido presentados como parte de las actas, y que en ellos se detallaban cuestiones pendientes y acuerdos informales celebrados durante las sesiones de auditoría.

7 de noviembre.

Según consta en las actas oficiales, sucedió lo siguiente:

- Una nueva revisión del modulo EMS que genera las Certificaciones de las máquinas de votación el día de las elecciones;
- Revisión permanente de la estructura de la base de datos;
- Revisión del archivo WEB.XML del servidor de aplicaciones JBoss

Notas y observaciones:

La primera página de esas actas contiene una observación, en la que se indica que una página con preguntas aún sin responder había sido presentada por un representante de la oposición como parte de las actas. Falta ese anexo en la copia de las actas que distribuyó el CNE.

8 de noviembre.

Según consta en las actas oficiales, sucedió lo siguiente:

- Mediante una herramienta denominada JARSIGNER, se generaron y registraron valores *hash* (MD5) de los archivos JAR de los componentes del módulo REIS y del Receptor de actas;

90 Los procedimientos del 30 de octubre constan en las actas del 31 de octubre, lo que convierte a este documento en un registro combinado de los procedimientos llevados a cabo durante los dos días.

91 La tabla es demasiado extensa para presentarla en el informe.

92 En las actas, no se aclaran detalles sobre estas "actualizaciones".

93 Señor Fidel Gil.

- Los partidos políticos solicitaron los *hashes* de los archivos de configuración finales de los objetos de la base de datos y del servidor de la aplicación JBoss. Se acordó fijar una fecha y hora para que los archivos definitivos, tal como serían utilizados en las elecciones, se pudieran "hashear".

21 de noviembre.

Según consta en las actas oficiales, se celebró una sesión de auditoria especial a fin de revisar los cambios de código fuente en los módulos REIS y Receptor de actas.[94] Los recursos en cuestión fueron "Error—messages.properties" y "language-ve.properties". Los archivos modificados se volvieron a "hashear" usando la herramienta JARSIGNER, y se registraron los valores *hash*.

30 de noviembre.

Se llevaron a cabo dos sesiones de auditoría, organizadas en respuesta a la necesidad de generar *hashes* de los archivos de configuración definitivos (véase 8 de noviembre). La sesión de la mañana tuvo lugar en el centro principal de datos del CNE (CNT1). Según las actas oficiales, se generaron y registraron *hashes* de los archivos de configuración de los siguientes componentes:

- Sistema de totalización completo (REIS, Receptor de actas, procesador de la base de datos);
- La base de datos propiamente dicha;
- La sesión de la tarde tuvo lugar en el centro de datos de contingencia del CNE (CNT2). Según las actas oficiales, se generaron los mismos *hashes*, se entregaron a los representantes de los partidos, y se llevó a cabo una revisión de las diferencias y similitudes entre el CNT1 y el CNT2 (y los *hashes* de sus archivos de configuración).

Notas y observaciones:

Los observadores del Centro Carter no fueron informados sobre la realización de esta serie de auditorías.

Auditoría de producción de las máquinas

Informe de observación	23/12/06
Observador	Ingo Boltz
Lugar de la auditoría	Filas de Mariche—Centro de AEROCAV de armado de las máquinas de votación, custodiado por los efectivos militares del Plan República
Objetivo de la auditoría	Seleccionar una muestra aleatoria del 0,5% de todas las máquinas de votación preparadas en el Centro de armado de AEROCAV, precintarlas y almacenarlas para la auditoria "pre-despacho" que se realizaría el domingo 26 de noviembre de 2006.
Organizaciones que participaron de la auditoría	Comando Miranda, Comando Rosales, Universidad Central de Venezuela, CNE (en adelante, denominados "los auditores")
Notas	Según Sergio Rivas, de la Universidad Central de Venezuela, esta auditoria se llevó a cabo todos los días de producción/armado de las máquinas, a partir del 1 de noviembre hasta la fecha (23 de noviembre). Cada uno de esos días se seleccionó el 0,5% de la producción del día, se precintó y se almacenó para ser auditada posteriormente.

94 No se indican los motivos para realizar estos cambios. Suponemos que el desarrollo y la reparación de errores del software del centro de totalización continuó hasta unos pocos días antes de las elecciones, lo que hizo necesario modificar el código fuente.

Descripción del procedimiento y observaciones:

1. Un operario del personal de armado de la planta presentó una lista de máquinas producidas desde la última auditoría de producción (el día anterior). La lista contiene tres IDs:

ID1: un número ID único consecutivo de la máquina (este número se utiliza principalmente para identificar la máquina a auditarse, y según Rivas es asignado por la UCV);

ID2: Otro número ID único ("CVA"), que contiene en un código numérico la futura ubicación geográfica de la máquina (estado, municipio, parroquia, centro de votación, "mesa" y "tomo"). Esta información está también detallada por escrito en la lista, véase ejemplo adjunto a este informe;

ID3: Otro "número de serie" para cada máquina (según Rivas, este número se utiliza principalmente en la logística de envíos de AEROCAV). (No se pudo determinar si este número se graba en la cubierta o simplemente se asigna).

2. Los auditores verificaron que la numeración consecutiva (ID1) fuera correcta, comparando el número producido desde la última auditoría con los números consecutivos de la lista;

3. Los auditores calcularon que el 0,5% de esa producción equivale a 1,91 máquinas; por lo tanto, se seleccionarían dos máquinas para la muestra;

4. Los auditores colocaron papelitos, cada uno con números que iban del #31990 al #32371, en una caja abierta de cartón. Los representantes de los comandos mezclaron los papelitos;

5. Los representantes de los partidos eligieron al azar, sin mirar dentro de la caja, uno de los papelitos. Los papeles que quedaron seleccionados fueron: #32371 y #32135;

6. Rivas registró este resultado en las actas, que fueron firmadas por los auditores (estas actas son para uso de la Universidad Central de Venezuela; el CNE lleva otras, las actas oficiales—véase más adelante). Rivas guardó las actas, un sobre con los papelitos que quedaban y los papeles seleccionados pegados al sobre para los registros de la Universidad;

7. Se le dijo a un miembro del personal del lugar que "vaya a buscar y prepare esas dos máquinas para su precintado." Los auditores no acompañaron personalmente a esa persona para asegurarse de que se retiraban esas dos máquinas de la línea de producción. (véanse otros comentarios más adelante);

8. Después de aproximadamente 15-20 minutos (estimativo), el personal del lugar volvió e informó que las máquinas estaban listas;

9. Los auditores ingresaron en el centro de producción propiamente dicho en grupo (la oficina del auditor está ubicada en un anexo del edificio). En la entrada, fueron registrados con un detector de metales por los efectivos militares del Plan República a cargo de la custodia del lugar. No se permitió el ingreso con teléfonos celulares ni con memorias extraíbles u otros objetos metálicos;

10. Los auditores fueron conducidos a una parte de la planta donde las máquinas estaban cargadas en camiones para su traslado. Allí los esperaban una paleta con las dos cajas que contenían las máquinas seleccionadas y dos cajas, separadas, para la boleta electrónica de las máquinas, en total cuatro cajas. Esas cajas supuestamente habían sido retiradas de la zona de armado por personal de la planta y habían sido colocadas allí para la auditoría;

11. Los auditores verificaron que los números que figuraban en la etiqueta pegada en las cajas coincidieran con los números seleccionados. No abrieron las cajas; los precintos de seguridad del CNE que tenían las cajas estaban intactos;

12. Después de constatar que la documentación de las cajas coincidía con los números seleccionados, los auditores acordaron que esas eran las cajas correctas, envolvieron la paleta con una lámina plástica y adjuntaron (con cinta adhesiva amarilla) cinco hojas de papel con detalles de la auditoria de ese día y las

firmas de los auditores, una a cada lado del "paquete" envuelto, a excepción de la cara inferior que quedó apoyada en la paleta y sin precintar (véanse comentarios más adelante);

13. Los auditores observaron que una carretilla elevadora tomaba la paleta y la colocaba en un estante alto de la zona de armado, donde se veían otras paletas envueltas y precintadas que correspondían a auditorias realizadas los días anteriores;

14. Se dijo que esta era la última auditoria de este tipo, dado que la producción había finalizado. La mayoría de los trabajadores estaban preparando máquinas de refuerzo (para reemplazar máquinas con fallas el día de las elecciones). Durante un día normal, el promedio de producción sería de 1500 unidades. Hoy, sólo se habían producido las mencionadas 382 unidades. Las máquinas de refuerzo no estaban entre aquellas de las cuales los auditores tomaron las dos máquinas de muestra; sólo seleccionaron entre las máquinas "estándar" que iban a ser enviadas a los centros de votación;

15. Los auditores se retiraron de la sala de producción (volvieron a pasar por un detector de metales a la salida) y regresaron a la oficina de auditoría;

16. Mientras tanto, en la oficina de auditoría, un funcionario del CNE había preparado las actas oficiales del CNE, que fueron leídas y firmadas por todos los auditores;

17. Los auditores se retiraron de las instalaciones.

Según una breve entrevista realizada al Director General de Informática del CNE, Leonardo Hernández, después de la auditoria, las máquinas que eran retiradas, precintadas y almacenadas para conformar la muestra se reemplazaban por clones idénticos y se enviaban al lugar que se había planificado. Estos clones se crean programando una máquina vacía con la configuración / información geográfica exacta de las máquinas que habían sido retiradas como muestra. No se indagó el tiempo que insumía el proceso de "clonación".

Comentarios:

No hubo duda de que los auditores eligieron dos máquinas "al azar", aun cuando el rigor estadístico de la metodología fue muy limitado. Hubo, sin embargo, dos cuestiones que generaron dudas:

Los auditores no supervisaron personalmente la recolección de las máquinas que habían elegido. Según Rivas, en elecciones anteriores y siguiendo los procedimientos de auditoria entonces válidos, los auditores sí eligieron números de máquinas, entraron personalmente a las instalaciones de producción, identificason las máquinas con los números correctos y supervisaron su traslado desde dichas instalaciones hasta el lugar donde fueron precintadas por los auditores. Sin embargo, a causa del gran número de auditores, se creó confusión y el proceso fue lento. Por lo tanto, al comienzo de este conjunto de auditorías (1º de noviembre), los auditores acordaron cambiar el procedimiento y confiar al personal de planta las tareas de buscar las máquinas y ubicarlas en la paleta, donde sus cajas serían luego inspeccionadas y precintadas.

Cuando se preguntó si la falta de supervisión personal no implicaba que podrían cambiarse las máquinas seleccionadas al azar por otras durante la "búsqueda y preparación de las máquinas de muestra" —no supervisadas—, se respondió que hacerlo no daría resultado dado que el software de cada máquina era único (ya que contenía información acerca de su ubicación exclusiva). Durante la auditoria "predespacho", cualquier discrepancia entre el ID único geocodificado registrado en las actas (ID1) y el ID1 de la máquina sería advertida.

La validez de ese argumento depende sin embargo de la velocidad a la que pueda crearse un "clon" (véase anteriormente). Si es posible tomar máquinas en blanco una vez que se conocen los números seleccionados, programarlas con la misma información geográfica que corresponde a las máquinas seleccionadas al azar por los auditores, colocarlas en cajas etiquetadas como las de las máquinas correctas y presentarlas para su auditoría —durante los 15-20 minutos durante los cuales los auditores esperaron

que se llevaran las máquinas y se presentaran para su precintado-, se les podría haber entregado a los auditores máquinas de reemplazo sin que lo supieran. Durante la posterior auditoria "pre-despacho" de esas máquinas de muestra, la discrepancia no se hubiera notado, dado que la información geográfica programada en cada máquina coincide con la registrada en las actas. Evidentemente, si se efectuara un reemplazo, auditar una máquina de muestra preparada especialmente, en lugar de una máquina seleccionada al azar del tipo de la que se despacha a todo el país, haría que la auditoría "pre-despacho" careciera de sentido.

Las paletas con las cajas no se precintaron completamente ya que la parte inferior quedó sin precintar. Aun si los problemas de velocidad (o el hecho de que el reemplazo tendría que efectuarse en medio de la operación de producción, con todo el personal de producción en las inmediaciones) impidieran una operación del tipo "reemplazo en caliente", resta saber si los precintos que se colocaron cumplirían su función. Dado que los precintos firmados no se sujetan directamente a las cajas, sino a la envoltura plástica que cubre el "paquete", sería posible reemplazar las máquinas después, en un momento más conveniente (por ejemplo, cuando no está el personal de planta) y con más tiempo para preparar los clones de las máquinas.

En el caso de las máquinas seleccionadas durante la presencia de los auditores en el lugar, la parte inferior de las dos cajas de cartón que quedó sin precintar podría haber sido abierta y se podrían haber reemplazado las máquinas sin violar los precintos.

En el caso de la mayoría de las *otras* paletas con las máquinas *previamente* seleccionadas y precintadas (que provenían de auditorías previas y que ya estaban almacenadas cuando se realizó la observación), resulta más difícil violar los precintos porque estaban dentro de cajas sumamente sólidas. Para poder cambiar las máquinas hubiera sido necesario quitar la envoltura plástica sin romperla (incluidos los precintos sobre esa envoltura plástica), reemplazar las cajas por otras y volver a colocar el plástico con los precintos intactos encima de las nuevas cajas.

Centro de control de tráfico de la red de CANTV

Fecha de observación	3/12/06
Observador	Ingo Boltz
Lugar de la auditoría	CANTV MiniCore—Centro de Control de Tráfico de Red para la Red Privada Virtual del CNE
Objetivo de la auditoría	Observar el tráfico de la red en la Red Privada Virtual del CNE (RPV, provista por CANTV) tal como se desarrolló durante la jornada electoral. Observar si hay tráfico entre las 16:00 (hora prevista para que las máquinas inicien la transmisión al servidor central de totalización) y observar cualquier posible actividad irregular de la red de allí en adelante.
Organizaciones presentes durante la observación	Comando Miranda, Comando empleados de CANTV

Si el "número de serie" de cada máquina (ID3) estuviera físicamente grabado en cada máquina de votación y fuera único, sería mucho más difícil llevar a la práctica ambos planes de reemplazo. De ser así, y si durante la auditoría pre-despacho se comparara el "número de serie" que consta en las actas con el "número de serie" de la máquina de votación auditada, una operación de reemplazo requeriría falsificar físicamente un número de serie de la máquina. Además, existirían dos máquinas con "números de serie" idénticos (uno en la muestra de la auditoria y otro en el lugar), lo que también debería ocultarse.

Descripción de las observaciones

El centro de control es un espacio de acceso restringido que se encuentra en las instalaciones de CANTV. El mismo cuenta con una serie de monitores para supervisar el funcionamiento de la red de CANTV. No está específicamente dedicado sólo a las operaciones del CNE. Se utiliza para controlar la totalidad de las operaciones de la red de CANTV.

Durante la observación, dos empleados de CANTV estaban cumpliendo tareas habituales (no relacionadas con el CNE), mientras que otros cuatro estaban supervisando la actividad en la Red Privada Virtual (RPV) que CANTV proveyó específicamente para el CNE.

La pantalla principal de observación (proyectada en una pared del fondo) contenía las ventanas siguientes:

1. Tráfico de Red por Router: Gráficos del desarrollo del trafico para cada uno de los routers principales de la RPV, con información prácticamente en tiempo real (5 minutos para actualización) sobre el tráfico en ese momento (amplitud de banda utilizada) tanto hacia como desde el router En todos los casos, había un router principal (1) y un router de contingencia (2).

Los routers fueron:

- 1 y 2 del CNE (router principal donde convergía todo el tráfico desde y hacia el CNE)
- Tráfico de líneas fijas 1 y 2 (*router* que recibía el tráfico proveniente de las máquinas de votación que transmitían mediante líneas telefónicas fijas)
- Tráfico por celulares MOVINET 1 y 2 (*router* que recibía el tráfico proveniente de las máquinas de votación que transmitían mediante teléfonos celulares)
- Tráfico satelital REDCOM 1y 2 (*router* que recibía el tráfico proveniente del centro de transmisión de contingencia que utiliza satélite)
- Centros de Autoridades Electorales Regionales (uno por cada estado)

2. Estadísticas RAS: Cantidad de módems en uso en determinado momento en diferentes RAS regionales.

3. Estadísticas de la cantidad de túneles y sesiones en uso en determinado momento

4. Imagen instantánea de las máquinas de votación que se comunican con el router del CNE en determinado momento

Tiempo de inactividad en segundos	IP asignado	Nombre de usuario de la máquina
"log_Machinecode@cnep2006.gob.ve"	…	23
"log_Machinecode@cnep2006.gob.ve"	…	12

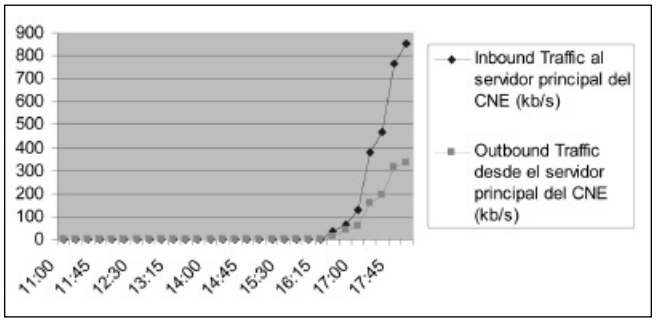
Cuadro 11.1: Fuente: información propia.

La observación comenzó una vez que el observador tuvo acceso al area MiniCore, aproximadamente a las 16:15. En ese momento, se visualizaba poco tráfico. Hubo intentos de conexión de máquinas de votación que intentaban conectarse pero el router del CNE no estaba asignando direcciones IP a las máquinas.

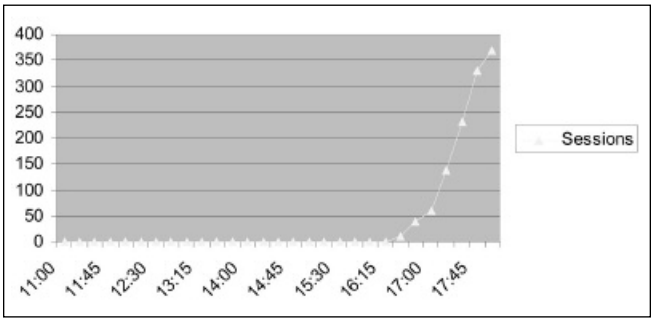
- Alrededor de las 16:30, el CNE comenzó a asignar direcciones IP y a aceptar comunicaciones, comenzando con aproximadamente 10 sesiones y un tráfico total de 37,4 kb/s en el router del CNE (entrante).
- Alrededor de las 16:45: 40 sesiones, con un tráfico total de 62.6 kb/s en el CNE (entrante),
- Alrededor de las 17:00: 60 sesiones, con un tráfico total de 130 kb/s en el CNE (entrante), 2 túneles
- Alrededor de las 17:20: 136 sesiones, con un tráfico total de 381 kb/s en el CNE (entrante); un tráfico total de 157 en el CNE (saliente), 4 túneles
- Alrededor de las 17:25: 232 sesiones, con un tráfico total de 465.9 kb/s en el CNE (entrante); tráfico total de 192.2 kb/s en el CNE (saliente), 5 túneles
- Alrededor de las 17:50: 330 sesiones, con un tráfico total de 767.3 kb/s en el CNE (entrante); un tráfico total de 313:8 kb/s en el CNE (saliente), 5 túneles
- Alrededor de las 18:15: 368 sesiones, con un tráfico total de 853.7 kb/s en el CNE (entrante); un tráfico total de 335:5 kb/s en el CNE (saliente), 5 túneles

Final prematuro de la observación

Poco después de tomar el último punto de datos, el observador advirtió que el tráfico en el gráfico correspondiente parecía emparejarse e incluso caer ligeramente. En ese momento debió ir al baño y por ende se vio forzado a abandonar el área MiniCore restringida. Al volver, no se le permitió el reingreso y no se le ofreció ninguna razón. **La observación no pudo completarse.**



Cuadro 11.2: Fuente: información propia.
Nota: En el gráfico de tráfico se registró un tráfico mínimo (alrededor de 1kb/s) en el router principal del CNE entre las 12:00 y las 16:00. Sin embargo no se estableció ninguna sesión. El personal de CANTV comentó que no estaba seguro acerca de qué era ese tráfico en la red, que se había enviado un informe al CNE y que el tema iba a ser investigado.



Cuadro 11.3: Fuente: información propia.

Anexo III
Declaracion del Centro Carter Sobre las Elecciones Venezolanas

NEWS
THE CARTER CENTER
ONE COPENHILL, ATLANTA, GA 30307

EL centro Carter Anuncia una Misión técnica para observar el proceso electoral en venezuela

16 de NOViembre 2006

para comunicación inmediata

Contactos:
En Caracas, Josefina Blanco 0416-6142848

En Atlanta, Deborah Hakes 404-420-5124

El Consejo Nacional Electoral invitó al Centro Carter a participar en la observación electoral internacional de las elecciones presidenciales pautadas para el tres de diciembre de 2006. Como respuesta a esta invitación, el Centro Carter anunció el envio de una misión limitada y de carácter técnico. Conforme a la Declaración de Principios de Observación Electoral, suscrita por más de 20 organismos internacionales en la sede de Naciones Unidas en Nueva York en octubre de 2005, las misiones electorales internacionales pueden ser de tipo integral, con el propósito de evaluar el proceso electoral en su totalidad, o de tipo limitado, enfocadas en aspectos específicos del proceso.

En este caso, la misión técnica del Centro Carter observará el uso de las tecnologías de votación automatizada en Venezuela a través de la participación en algunas de las auditorias y simulacros patrocinados por el CNE. La misión constará de dos grupos de trabajo: uno, conformado por dos expertos, que trabajarán en Caracas a partir del 20 de noviembre; y otro conformado por un equipo de especialistas que realizará una observación de corta duración en los días anteriores y posteriores al 3 de diciembre.

Dado su carácter limitado, y su corta duración, la Misión no producirá una evaluación integral del proceso electoral, ni una evaluación extensiva de la integridad del sistema de votación automatizado. No obstante, luego de las elecciones, la misión emitirá un informe en donde se describirán los componentes y el funcionamiento del sistema venezolano durante este proceso, utilizando para ello una perspectiva comparativa con el funcionamiento de otros sistemas de votación automatizada en diversos países. La misión ofrecerá asimismo posibles recomendaciones.

La misión pretende asimismo contribuir con un proyecto más amplia del Centro Carter para el desarrollo y actualización de una metodología para la observación y evaluación de sistemas de votación automatizada en el mundo, proyecto actualmente desarrollado en colaboración con otras organizaciones internacionales.

El Centro Carter fue fundado en 1982 por el ex Presidente de los Estados Unidos Jimmy Carter y su esposa, Rosalynn, en colaboración con la Universidad de Emory, para avanzar la paz y la salud mundial. Una organización sin fines de lucro y no gubernamental, el Centro Carter ha ayudado a mejorar la vida para personas en más de 65 países a través de resolviendo conflictos; avanzando la democracia, los derechos humanos, y oportunidades económicas; previniendo enfermedades; mejorando la asistencia de salud mental; y enseñando a los campesinos como aumentar el cosecho. Para conseguir más información sobre el Centro Carter, visite www.cartercenter.org

Anexo IV
Baseline Survey for Electronic Voting Systems

Draft

May 2007

The information gathered by answering these questions should create a comprehensive picture of the voting system in use and thus allow a more full assessment of its use.

Information should be gathered through review of appropriate legislation, decrees, bylaws and rules, and interviews with election administration officials, technical and legal experts, representatives of political parties, and domestic observation and civil society organizations.

Any supporting documentation should be retained including the elections law, certification procedures, standards against which the technology is measured, reports on past processes, and so forth. Be sure to include details about how, where, and when the information was obtained, and, particularly in the case of interviews, the name, title, and affiliation of the source of the data. This process likely will occur over a number of weeks in the months leading to election day.

After collecting as much data as possible regarding the use of the electronic voting system, a synopsis of your findings will be written. This synopsis will provide an overview of the system that can be used by other observers as a point of reference. In addition, data collected will be used to modify more generic election day and other checklists to capture information on the actual functioning of the system.

Technology Overview

1. Which types of voting system technology are used?
   a. Direct recording equipment (DRE)
   b. Precinct count optical scan equipment
   c. Central count optical scan equipment
   d. Lever machines
   e. Electronic poll book
   f. Ballot marking devices

2. Are these technologies used throughout the country? If no, please attach maps indicating where different technologies are used.

3. What version or versions of all hardware, software, and firmware components are deployed in the voting system technologies, including but not limited to any version of the following:
   a. Smart card devices
   b. Firmware used in touch screens
   c. Vote counting server
   d. Other (please describe)

Note. The Carter Center would like to acknowledge the Verified Voting Foundation (www.verifiedvoting.org), the work of which informed the Center's methodology.

4. Is this the first time these technologies have been used?

5. If no, how long have e-voting systems been used? In which previous elections were they used? Please provide separate reviews of previous elections.

6. Are there any documents available to the public containing information on the version numbers, makes, models, and functional status of these technologies? If so, please attach any relevant reports.

7. Does the technology produce a voter verified paper trail? If yes, please describe how it works.

8. Is the voter able to verify that the paper ballot matched his or her choice *before* the vote is cast?

9. Describe what happens to the paper trail during and after voting.

10. Provide an overview of the institutions responsible for the administration of the electronic voting systems, including the vendor, any certification or testing bodies, and organizations responsible for maintenance or election official training.

11. Do these organizations provide checks and balances on one another? If so, please explain how they do so.

12. Please include a diagram, detailed descriptions and, where possible, photographs of the election office components; how they are connected to one another; and their respective roles in the election process.

13. Provide detailed descriptions of the devices used in each polling place (e.g., DREs, supervisor's cards, voter's cards, memory cards), including physical descriptions, photos (if possible), descriptions of how they work, and when and how they interact with one another.

14. Please include a detailed diagram and description of how the different technologies used are networked.

Legal Framework

15. Is the use of electronic voting technologies anticipated in the current electoral legislation (or other binding legislation) or has it been introduced via subsequent decree, regulations, or other ad hoc measures?

16. Does the legal framework prescribe the type of electronic technology that is used? If so, please describe, including any outlined objectives for the introduction of this technology.

17. Does the law (legislation or subsequent decisions, decrees, and regulations) provide for transparency promotion measures, such as the use of an independent certification body and pre- and postelection audits that are open to party agents and observers? If so, please describe and indicate whether, in your opinion, access of party agents and observers to the audit process appears adequate.

18. Does the law (legislation or subsequent decisions, decrees, and regulations) require that appropriate technical steps be taken to ensure that the secrecy of the vote is guaranteed (for example, measures to ensure that the voting sequence cannot be reconstructed or that the votes cast cannot be tied to a specific voter)?

19. Does the law (legislation or subsequent decisions, decrees, and regulations) clearly outline the roles and responsibilities of public authorities, independent bodies, and vendors? Please describe.

20. Does the law (legislation or subsequent decisions, decrees, and regulations) provide a framework for contractual obligations between the state and the vendor or the independent certification bodies that is unique from standard contract law? Please describe the regulatory framework for these relationships.

21. Does the law (legislation or subsequent decisions, decrees, and regulations) make special provision for complaints and remedial actions based on the use of electronic technologies? Please provide a detailed description of the provisions and how they are related to the standard complaints procedures.

22. Do electoral offense provisions of the electoral law also apply to the new technologies in use?

Technology Vendors and Procurement of Equipment

23. If e-voting systems have been recently introduced, why were they introduced?

24. Who designed and developed the electronic voting system? Was the technology designed by the state or the vendor?

25. What vendors provide which components of the electronic voting systems? Please describe.

26. Is the technology leased or purchased?

27. Have the above vendors made contributions to political parties or campaigns? If so, please describe and attach any relevant documentation.

28. At what level was the procurement process of this technology initiated and conducted?

29. Was the vendor chosen through a transparent and competitive process? Please describe and attach any supporting documentation.

30. What reasons were given by those responsible for this choice of technology?

31. Are any of the following services included in the contract with the vendor? If so, please explain in greater detail.

    a. Timely supply of equipment
    b. Pre- and postelection testing
    c. Regular physical maintenance
    d. Regular software upgrades
    e. Replacement of equipment in case of failure
    f. Ballot design
    g. Ballot printing
    h. Warranties
    i. Other (please describe)

32. What, if any, penalty or reimbursement provisions are triggered by technical problems with the technology?

Certification, Testing, and Security of the System

Voter Verified Paper Trails (VVPT)

33. If the machine produces a VVPT, is the voter able to verify that the paper ballot matched his or her choice *before* the vote is cast?

34. What happens to the paper trail during and after voting?

35. Do rules and regulations ensure that the VVPT does not undermine the secrecy of the ballot and that voters are not able to remove evidence of how they voted from the polling station?

Certification

36. Is certification of the voting technology required by law (legislation or subsequent decisions, decrees, and regulations)?

37. What is the certification process? Please describe the process in detail, including the relationships between the different certification processes, and attach any relevant documentation.

38. Who is responsible for this certification?

39. Who pays for the certification of the technology?

40. What is the relationship between the certification body and the organization whose technology is being certified?

41. Does certification occur before or after the procurement process?

42. Is the certification process accessible to the public, political party agents, domestic observers, or international observers?

43. What standards are applied to the certification of e-voting technologies? Please attach relevant documentation.

44. Is the technology recertified after every upgrade and repair?

45. In your opinion, after systematic review, what are the weaknesses of the certification standards?

Acceptance Testing

46. Does the law require that acceptance testing take place?

47. Which components of the system undergo acceptance testing?

48. What does acceptance testing include? Please describe.

49. Who is responsible for acceptance testing?

50. Who designs the acceptance tests?

51. How often and when do acceptance tests occur?

52. Who pays for acceptance testing?

53. Who has access to the acceptance tests?
    a. General public
    b. Political party agents
    c. Domestic observers
    d. International observers

54. Under what conditions are acceptance tests conducted?

Pre-election Testing

55. Does the law (legislation or subsequent decisions, decrees, and regulations) require that pre-election testing take place?

56. Who is responsible for pre-election testing and does the law (legislation or subsequent decisions, decrees, and regulations) require that the equipment is tested publicly and by an independent body? Please explain these procedures, including who is allowed to observe testing.

57. Does the state have recommended procedures for the testing and use of each type of election equipment? If so, please describe these procedures and attach any supporting documentation.

58. Who designed the pre-election tests?

59. Who conducts the pre-election tests?

60. How many machines are tested? Please provide details of the sampling method used to conduct the pre-election tests.

61. What is the timetable for pre-election tests and where are they conducted (in a central location, provincial locations, or elsewhere)? Please provide further details and any relevant documentation.

62. Is equipment retested after every upgrade and repair? If not, why?

63. Are pre-election tests open to the general public, political party agents, domestic observers, or international observers? Please attach relevant documentation.

64. Is all voting equipment tested upon delivery from voting technology vendors?

65. Does the law (legislation or subsequent decisions, decrees, and regulations) require that pre-election testing include the following?
    a. Testing the power-up of every machine
    b. Simulation of likely voting orders, patterns, and ranges

c. Stress-testing with large numbers of votes
d. Checking vote tally
e. Testing correct date and time information
f. Testing date set to election day run-throughs
g. Simulations of error conditions to evaluate system response to problems and mistakes
h. Testing reboot and restart functionality
i. Testing equipment recovery from system crashes
j. Testing for unexplained flashing or otherwise inconsistent or potentially suspicious behavior
k. Checking for complete list of candidate names, party affiliations, ballot initiatives, or proposition options
l. Testing the use of an independent log to compare the system count and the selections made by the voter
m. Testing the use of an independent log to compare the paper ballots (if used) produced with the system count and the selections made by the voter
n. Testing of display calibration
o. Testing of audio ballot functionality
p. Testing of the security and authentication techniques used in connecting the voting machines to the network (if applicable)
q. Testing to ensure that the ballot information for each precinct is correct
r. Other (please describe)

66. Please provide any relevant documentation outlining the regulations and procedures for pre-election testing.

Election Day Testing

67. What tests or audits, if any, are required on election day? Please describe in detail and attach any relevant documentation outlining regulations and procedures for election day auditing or testing.

Physical Security of the System

68. Please provide a detailed description of the technologies in place to ensure the physical security of the electronic voting system (e.g., tamper-evident seals).

69. Who is allowed physical access to the equipment, and what measures are taken to prevent physical tampering with election equipment?

70. Is physical access documented? If so, who maintains these records?

71. Are vendors permitted access to the voting systems after they have been delivered? If so, for what purposes and when are they permitted access? Is this access controlled and documented?

72. What happens if a machine is found to have been tampered with? Please describe any contingency plans for such an event.

73. Who is responsible for transporting the machines from their storage location to testing centers and polling places? Please provide relevant documentation.

74. Is the chain of custody during the transportation process documented? If so, who maintains those records?

75. When will transportation of the equipment take place?

76. Who pays for the transportation of the equipment?

Security and Integrity of the System

77. Are records kept of all upgrades and repairs made to voting equipment?

78. Is any equipment used for a purpose other than election administration? If so, please provide further details of the other uses of the equipment, including the purpose, how people have physical access, other software that is required for this secondary use, and so forth.

79. Which components of the system are stored in escrow?

80. Are there written procedures and requirements regarding the storage of voting system software stored in escrow? If so, please provide further details on these requirements and the people who have access to the software.

81. Is there a cutoff date after which no further changes or updates may be made to the voting system? What is that date?

82. Please provide a detailed description and diagram of all of the data paths in and out of the components of the system.

83. How is access to the data ports secured when the equipment is not in use?

84. What is the method of transmission of information between the technologies? Please describe.

85. How are transmissions secured from alteration and interference? Please provide a detailed description.

Software

86. Is any of the voting system software open source software? If yes, please include information on location and availability.

87. Who is responsible for inspecting the software used in the electronic system?

88. Under what conditions does the official software inspection take place? Please provide a detailed description of the software inspection process, including the length of time allotted for the inspection and the means of inspection.

89. Does the law (legislation or subsequent decisions, decrees, and regulations) allow independent inspection of the software? Please provide further details, including any pertinent reports that might be available.

90. Under what conditions are independent software inspections (including representatives of political parties and civil society) conducted? Please provide a detailed description of the inspection process, including the length of time allotted for the inspection and the tools inspectors are allowed to use.

91. Does the software inspection (either by an independent body or the official organization responsible) include checking the source code against the executable code?

92. Who is responsible for creating the executable code from the source code, and is this process subject to independent verification?

93. Is any extraneous software installed on the servers? If so, please provide further information about this software and its use.

Central Tabulating Computer

94. Who has physical access to the central tabulating computer, and what measures are taken to prevent physical tampering with election equipment?

95. Is physical access documented? If so, who maintains these records?

96. Are vendors permitted access to the central tabulating computer? If so, for what purposes and when are they permitted access? Is this access controlled and documented?

97. Are records maintained of all upgrades and repairs made to the central tabulating computer?

98. Is the central tabulating computer used for any purpose other than election administration? If so, please provide further details of the other uses of the equipment, including the purpose, the people who have physical access, other software that is required for this secondary use, and so forth.

99. Are there procedures in place that encourage independent verification of the transmission of data (such as printing of polling place election results prior to transmission to the central tabulating computer, which can be compared to the final or interim results)?

100. When is this computer networked to the other hardware in use?

101. Please describe in detail and provide diagrams of all of the data paths into and out of the central tabulating computer.

102. Is the transmission of information between the central tabulating computer and other equipment secure from any outside intervention or hacking? Please describe security measures in place.

103. What contingency plans are in place in the event of failure of the central tabulating computer? Please describe.

Electronic Poll Books and Voter Identification

104. If electronic poll books are used, who is responsible for creating the database that is used and who has access to that database throughout the electoral process?

105. Is there an independent review of the electronic poll book database? If so, by whom?

106. Is the voter roll database connected to any other databases (e.g., databases of biometric data) ?

Ballot Building

107. Who is responsible for building the electronic ballots?

108. Is there independent review of the database from which the ballot is built?

109. Are there official guidelines or regulations for ballot building? Please attach if available.

110. What is the process for building ballots? Please provide a detailed description of this process.

111. Does the electronic ballot replicate the paper ballot in layout, candidate order, and design?

Public Confidence in Electronic Voting Technologies

112. Are civil society organizations reporting on issues related to electronic voting? If so, please attach any pertinent documentation.

113. Are the media reporting on issues related to electronic voting? If so, please provide a sample of relevant stories.

114. Are simulations of the opening, voting, closing, and counting procedures provided and open to the public? If so, please provide further information about location, timing, and attendance of the simulations.

115. Are there public information drives about the use of electronic voting?

116. Have voters, political party agents, domestic observers, or others received training on the electronic system in use?

117. Have any opinion polls been conducted related to the use of electronic election technology? If so, please attach any available results reports.

118. In your opinion, does there appear to be a sense of concern among the general public about the transparency of electronic voting systems? If so, has the state responded to these concerns? Please explain.

119. Were political parties consulted during the technology procurement process?

120. Are there any political parties or individual candidates who are campaigning on issues related to the use of electronic voting? Please provide further details.

Accessibility

121. Are ballots available in minority languages?

122. Do voters in the following circumstances use electronic voting technologies to cast their ballots? (Circle all that apply)

    a. Confined to a hospital
    b. Confined to home
    c. In prison
    d. Outside electoral district on election day

123. Does this equipment undergo the same testing as the equipment deployed to polling places?

124. Is provision made for voters who are disabled or illiterate?

125. If the machines produce a voter verified paper trail, does the paper ballot appear in such a format that it is clear to illiterate or disabled voters that their vote has been correctly cast?

Election Day Procedures

126. Please describe the intricacies of election day procedures as specified by the election law or the rules and regulations of the electoral management body, including the following:

    a. Poll opening and setup of all equipment (including production of zero tape, ensuring that all items are present and accounted for)
    b. Connectivity of equipment during the course of the day (including when, why, and how long the machines are connected to a network and what security and authentication measures are in place)
    c. Voting process
    d. Storage of spare equipment
    e. Poll closing procedures
    f. Vote counting and tabulation procedures
    g. Storage and transportation of polling place results

127. Can a voter spoil his or her ballot? If so, how? Please describe how a vote can be spoiled and what happens to spoiled ballots.

128. Can a voter cancel his or her vote prior to casting the ballot? If yes, what is the process of cancellation?

Contingency Planning

129. Does the law or official rules and regulations require the following?

    a. Contingency plans are in place in case of equipment failure.

b. Replacement equipment is available in the event of malfunctions. If so, is this replacement equipment the same model as the technology it replaces? Is it deployed from a central location or kept at each polling place? (Please describe)
c. Substitute technology is subject to the same testing and evaluation procedures as equipment originally deployed to polling places.
d. Chain-of-custody procedures are in place for equipment taken out of service during an election. If so, is this chain of custody documented and are any of these documents available to the public?
e. A process for documenting malfunctions, failures, or errors is in place.
f. A process for obtaining election day performance records (e.g., errors and malfunctions) of specific equipment is in place.
g. Contingency plans and procedures for partial or total power outage are in place.

130. What contingency planning training is in place for polling officials? Please describe and attach any pertinent information.

131. How do polling places and central offices communicate in case of emergencies, such as power outages, telecommunications failure, and so forth?

Ballot Counting and Recount and Complaint Procedures

132. How are ballots counted at the end of the election? Please describe.

133. Are results printed and publicized prior to their transmission to the central tabulation system?

134. Are paper ballots counted at the end of election day? If so, is the tally compared to the electronic result tally produced by the voting machine?

135. Are paper ballots from all machines counted, or is this process conducted on a statistical sample? If so, what sampling method is used?

136. What procedures are in place if there is a discrepancy between the paper ballot count and the electronic tally?

137. What triggers a recount?

a. Voter application
b. Candidate application
c. Narrow margin of victory
d. Automatic random recount
e. None of the above
f. Other (please describe)

138. Can a recount be requested regardless of the margin of victory?

139. Who is financially responsible for the cost of a recount? Please provide further information, including whether an individual, if financially responsible, can seek reimbursement for the cost.

140. Are paper or electronic ballots recounted? If paper ballots are recounted, were these ballots verified by the voter? Please provide a detailed description of this process.

141. What voting records are maintained?

    a. Paper ballots
    b. Electronic records stored in the hard drive or disk on module (DOM) of the machine
    c. Electronic records produced by the modem
    d. Records maintained in a secondary memory device

142. If multiple records are maintained, are these reconciled as part of the counting or recounting process? If yes, please describe.

143. In case of discrepancy, what is the ballot of record? Please provide further details.

144. Have past election results been disputed because of the use of electronic voting technologies? If so, please attach a summary of the complaint, its resolution, and any related procedural or legislative changes regarding the use of electronic voting technologies that followed.

Anexo V
Poll Opening Observation Form
Venezuela 2006

Instructions:
If you cannot answer the question because you have not observed this aspect of the electoral process, please circle N/O—Not Observed. If the question is not relevant, please circle N/A. If you answered "no" to any asterisked (*) question or irregularities occurred, please provide details on the back of the form.

When possible, ask domestic observers and political party agents for their observations during the period prior to your arrival. When applicable, fill out both the "Direct Observation" and the "Reported to Our Observers" columns, even if the responses are different.

Polling Station No.: _____

Team No.: _____ Time of Arrival: _____

City/District: _____ Time of Departure: _____

Province: _____ Date: _____

1. What technology is used in this polling station?

a. Smartmatic SAES 3000 voting machine (small DRE)	
b. Smartmatic SAES 3300 voting machine (larger DRE)	

2. How many machines are located in this polling station? _____

3. What is the number of registered voters in this polling station? _____

4. Where were these machines stored immediately prior to the election?

_____

_____

5. When did the equipment arrive at the polling station?

_____

_____

6. Who delivered the equipment to the polling station?

_____

_____

7. Was this chain of custody documented? Yes No

8. If yes, who maintains the documentation?

_____

_____

Poll Opening

	Direct Observation		Reported to Our Observers		Not Observed or Not Applicable	
9. Are electronic voting machines positioned:						
a. With enough distance between them, at such an angle, and with shields to ensure privacy?	Yes	No	Yes	No	N/O	N/A
b. To plug into an electrical outlet?*	Yes	No	Yes	No	N/O	N/A
10. Are the polling officials and support technicians properly accredited and identified?*	Yes	No	Yes	No	N/O	N/A
11. Did the polling officials perform diagnostics and print the diagnostic report for all machines?*	Yes	No	Yes	No	N/O	N/A
12. Was the setup of the machines completed without problems?* (If yes, skip to question 13)	Yes	No	Yes	No	N/O	N/A
a. If no, could the polling station technicians resolve the problem within the specified 30 minutes?	Yes	No	Yes	No	N/O	N/A
b. If technicians could not resolve the problem, was the machine replaced with another machine within the maximum of 120 minutes (counting from occurrence of the problem)?	Yes	No	Yes	No	N/O	N/A

	Direct Observation		Reported to Our Observers		Not Observed or Not Applicable	
c. If the machine was not replaced within 120 minutes, did the polling station change to manual voting?*	Yes	No	Yes	No	N/O	N/A
13. Did you observe the machines to be free from any irregular interference such as the connection of an external keyboard or any other device (except the standard release button or the standard ballot tablet)?	Yes	No	Yes	No	N/O	N/A
14. Before voting began, did each machine produce a zero tape? * (*Acta cero*)	Yes	No	Yes	No	N/O	N/A
15. Did the polling officials store the diagnostic reports and the zero tapes in the supplied envelopes?	Yes	No	Yes	No	N/O	N/A
16. Did polling officials log the identification number of each machine as it was opened and prepared for the election?*	Yes	No	Yes	No	N/O	N/A
17. Did you observe the official tamper-proof tape that sealed the case in which the voting machines arrived?*	Yes	No	Yes	No	N/O	N/A
18. Did the case contain all the required machine components?*	Yes	No	Yes	No	N/O	N/A
19. Did you observe tamper-proof seals or tape covering the ports of the machines prior to their setup?*	Yes	No	Yes	No	N/O	N/A
20. Did polling staff receive all equipment needed?*	Yes	No	Yes	No	N/O	N/A
21. If applicable, did polling staff receive an adequate number of paper ballots in case of failure of the machines?*	Yes	No	Yes	No	N/O	N/A
22. Are the machines set up so as to be accessible to disabled voters who may need special equipment, be in a wheelchair, or have other restrictions on their movement?	Yes	No	Yes	No	N/O	N/A
23. Did polls open on time?	Yes	No	Yes	No	N/O	N/A

Poll Opening — Electronic Poll Book Observation

	Direct Observation		Reported to Our Observers		Not Observed or Not Applicable	
24. Is the automated fingerprint system going to be used at the polling station? (Fingerprint system—SAV/*Captahuellas*)	Yes	No	Yes	No	N/O	N/A
25. Was the fingerprint system set up without problems?*	Yes	No	Yes	No	N/O	N/A

Comments

Anexo VI
Election Day Observation Form
Venezuela 2006

Instructions:
If you cannot answer the question because you have not observed this aspect of the electoral process, please circle N/O—Not Observed. If the question is not relevant, please circle N/A. If you answered "no" to any asterisked (*) question or irregularities occurred, please provide details on the back of the form.

When possible, ask domestic observers and political party agents for their observations during the period prior to your arrival. When applicable, fill out both the "Direct Observation" and the "Reported to Our Observers" columns, even if the responses are different.

Polling Station No.: _____
Team No.: _____ Time of Arrival: _____
City/District: _____ Time of Departure: _____
Province: _____ Date: _____

1. What technology is used in this polling station?

a. Smartmatic SAES 3000 voting machine (small DRE)	
b. Smartmatic SAES 3300 voting machine (larger DRE)	

2. How many machines are located in this polling station? _____

3. What is the number of registered voters in this polling station? _____

4. Where were these machines stored immediately prior to the election?

_____

_____

5. When did the equipment arrive at the polling station?

_____

_____

6. Who delivered the equipment to the polling station?

_____

_____

7. Was this chain of custody documented? Yes No

8. If yes, who maintains the documentation?

_____

_____

After Polls Open

		Direct Observation		Reported to Our Observers		Not Observed or Not Applicable	
9.	Do electronic ballots seem complete and contain all appropriate candidates and races?*	Yes	No	Yes	No	N/O	N/A
10.	Do the screens appear to be properly calibrated?*	Yes	No	Yes	No	N/O	N/A
11.	Do electronic ballots appear to be operating properly?*	Yes	No	Yes	No	N/O	N/A
12.	Does the ballot touchpad appear to be properly calibrated?*	Yes	No	Yes	No	N/O	N/A
13.	Are voters on electronic systems made aware by the machine that they might be undervoting?*	Yes	No	Yes	No	N/O	N/A
14.	Do voters seem to find the instructions for casting a ballot clear?*	Yes	No	Yes	No	N/O	N/A
15.	Do accessibility devices appear to be working properly?*	Yes	No	Yes	No	N/O	N/A
16.	Do election officials keep a running tally on a regular basis through the day to ensure the number of votes on the machine is consistent with the number of people who have voted?	Yes	No	Yes	No	N/O	N/A

	Direct Observation		Reported to Our Observers		Not Observed or Not Applicable	
17. Are paper ballot receipts handled according to the established procedure?*	Yes	No	Yes	No	N/O	N/A
18. Are the machines' ports physically closed and inaccessible during voting?	Yes	No	Yes	No	N/O	N/A
19. Is the equipment free from network connectivity throughout your observation?*	Yes	No	Yes	No	N/O	N/A
Handling Exceptions — Please Address the Following Questions to Polling Officials						
20. Are poll workers aware of contingency plans in case of equipment or system failure?*	Yes	No	Yes	No	N/O	N/A
21. Is replacement voting equipment (machines, cards, card programmers, etc.) available in the event of failure?*	Yes	No	Yes	No	N/O	N/A
22. Is the same equipment set up at poll opening used throughout the day?*	Yes	No	Yes	No	N/O	N/A
23. If no, is the chain of custody for the removed equipment documented?*	Yes	No	Yes	No	N/O	N/A
24. If voting equipment is taken out of service during election day, are votes and other relevant information extracted from it?*	Yes	No	Yes	No	N/O	N/A
25. Is there documentation outlining the failure that has occurred and recording the chain of custody for:						
a. The machine?*	Yes	No	Yes	No	N/O	N/A
b. The information drawn from the machine?*	Yes	No	Yes	No	N/O	N/A
26. In case of power loss can the equipment operate on a battery?*	Yes	No	Yes	No	N/O	N/A
27. If yes, do polling officials:						
a. Have sufficient batteries?*	Yes	No	Yes	No	N/O	N/A
b. Know the average life of the battery?*	Yes	No	Yes	No	N/O	N/A

Polling Station Officials

	Direct Observation		Reported to Our Observers		Not Observed or Not Applicable	
28. Have polling station officials received training specific to the equipment in use, including trouble-shooting in case of technical difficulties?*	Yes	No	Yes	No	N/O	N/A
29. Are polling station officials adequately instructing voters on the method for casting their ballots?	Yes	No	Yes	No	N/O	N/A

Election Day Auditing

30. Did polling officials conduct parallel testing?*	Yes	No	Yes	No	N/O	N/A

Comments

Anexo VII
Poll Closing Observation Form
Venezuela 2006

Instructions:
If you cannot answer the question because you have not observed this aspect of the electoral process, please circle N/O—Not Observed. If the question is not relevant, please circle N/A. If you answered "no" to any asterisked (*) question or irregularities occurred, please provide details on the back of the form.

When possible, ask domestic observers and political party agents for their observations during the period prior to your arrival. When applicable, fill out both the "Direct Observation" and the "Reported to Our Observers" columns, even if the responses are different.

Polling Station No.: _____

Team No.: _____ Time of Arrival: _____

City/District: _____ Time of Departure: _____

Province: _____ Date: _____

1. What technology is used in this polling station?

a. Smartmatic SAES 3000 voting machine (small DRE)	
b. Smartmatic SAES 3300 voting machine (larger DRE)	

2. Which communication method is being used in this polling station?
   a. Fixed-line telephone ☐
   b. Cellular telephone ☐
   c. Satellite telephone ☐
   d. No transmission, but transport of memory stick to nearest transmission center ☐
   To which center? _____

3. How many machines are located in this polling station? _____

4. What is the number of registered voters in this polling station? _____

5. Where were these machines stored immediately prior to the election?
   _____
   _____

6. When did the equipment arrive at the polling station?
   _____
   _____

7. Who delivered the equipment to the polling station?
   _____
   _____

8. Was this chain of custody documented? Yes No

9. If yes, who maintains the documentation?
   _____
   _____

Poll Closing

	Direct Observation		Reported to Our Observers		Not Observed or Not Applicable	
10. Once voting has finished for the day, do poll workers follow procedures to complete the process and close the polls?*	Yes	No	Yes	No	N/O	N/A
11. Is the memory card containing the voted ballots removed from the port?	Yes	No	Yes	No	N/O	N/A
12. Were the polling place totals successfully printed?*	Yes	No	Yes	No	N/O	N/A
13. If not, were the proper contingency procedures followed?*	Yes	No	Yes	No	N/O	N/A
14. Do polling officials print polling place totals before sending any electronic communications out of the polling place via connection to a network?	Yes	No	Yes	No	N/O	N/A

	Direct Observation		Reported to Our Observers		Not Observed or Not Applicable	
15. Was the transmission method as originally planned for this polling station used?	Yes	No	Yes	No	N/O	N/A
16. Did the transmission to the central tally server complete?*	Yes	No	Yes	No	N/O	N/A
17. Was transmission successful at first attempt?*	Yes	No	Yes	No	N/O	N/A
18. If transmission was not performed locally and the memory sticks were transported to the nearest transmission center, were the prescribed security measures followed?*	Yes	No	Yes	No	N/O	N/A
19. Is a copy of the printed polling place totals available for public review at the end of the day?*	Yes	No	Yes	No	N/O	N/A
20. Were copies of the electronic tallies printed for all party observers (nine in total)?	Yes	No	Yes	No	N/O	N/A
21. Was public access to the audit process free from intervention by the military or other government authority?*	Yes	No	Yes	No	N/O	N/A
22. Do election officials appear to understand and adhere to the required procedures?*	Yes	No	Yes	No	N/O	N/A
23. Were there any complaints arising from the use of election equipment? If so, please provide details, including their resolution.	Yes	No	Yes	No	N/O	N/A

Election Day Auditing

24. Was a hot audit conducted? Yes No

25. Who conducted the hot audit?

_____

_____

_____

26. How many machines in your polling place were audited?

_____

_____

_____

27. How were the machines selected to be audited?

_____
_____
_____
_____

28. If an unofficial comparison of the count of the paper receipts with the electronic tally of the votes took place, did they match? If no, please explain what happened and how polling officials explained the discrepancy.

_____
_____
_____

Postelection Custody and Security

	Direct Observation		Reported to Our Observers		Not Observed or Not Applicable	
29. Are all removable memory devices removed from the equipment?	Yes	No	Yes	No	N/O	N/A
30. Is there a clear and documented chain of custody for the equipment and the saved data?*	Yes	No	Yes	No	N/O	N/A
31. Is all equipment appropriately secured in preparation for storage until the next election?*	Yes	No	Yes	No	N/O	N/A

Comments

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

The Carter Center at a Glance

Overview: The Carter Center was founded in 1982 by former U.S. President Jimmy Carter and his wife, Rosalynn, in partnership with Emory University, to advance peace and health worldwide. A non-governmental organization, the Center has helped to improve life for people in more than 65 countries by resolving conflicts; advancing democracy, human rights, and economic opportunity; preventing diseases; improving mental health care; and teaching farmers to increase crop production.

Accomplishments: The Center has observed 67 elections in 26 countries; helped farmers double or triple grain production in 15 African countries; worked to prevent and resolve civil and international conflicts worldwide; intervened to prevent unnecessary diseases in Latin America and Africa; and strived to diminish the stigma against mental illnesses.

Budget: $49.1 million 2005–2006 operating budget.

Donations: The Center is a 501(c)(3) charitable organization, financed by private donations from individuals, foundations, corporations, and international development assistance agencies. Contributions by U.S. citizens and companies are tax-deductible as allowed by law.

Facilities: The nondenominational Cecil B. Day Chapel and other facilities are available for weddings, corporate retreats and meetings, and other special events. For information, (404) 420-5112.

Location: In a 35-acre park, about 1.5 miles east of downtown Atlanta. The Jimmy Carter Library and Museum, which adjoins the Center, is owned and operated by the National Archives and Records Administration and is open to the public. (404) 865-7101.

Staff: 160 employees, based primarily in Atlanta.

Martin Frank

THE
CARTER CENTER

The Carter Center

One Copenhill
453 Freedom Parkway
Atlanta, GA 30307
(404) 420-5100 ◆ Fax (404) 420-5145

www.cartercenter.org